



# **THE STATUS OF ENTERPRISE ARCHITECTURE AND INFORMATION TECHNOLOGY INVESTMENT MANAGEMENT IN THE DEPARTMENT OF JUSTICE**

U.S. Department of Justice  
Office of the Inspector General  
Audit Division

Audit Report 06-02  
November 2005

# **THE STATUS OF ENTERPRISE ARCHITECTURE AND INFORMATION TECHNOLOGY INVESTMENT MANAGEMENT IN THE DEPARTMENT OF JUSTICE**

## **EXECUTIVE SUMMARY**

To more effectively manage its Information Technology (IT) investments in compliance with legislation and regulations, the Department of Justice (Department) is in the early stages of developing Enterprise Architecture and Information Technology Investment Management (ITIM) processes. An Enterprise Architecture is a strategic information asset base that defines the organization's mission, the information and technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs. Enterprise Architectures provide explicit structural frames of reference that allow an understanding of: (1) what the enterprise does; (2) when, where, how, and why it does it; and (3) what it uses to do it. An ITIM process enables an organization to manage its IT investments by continuous identification, selection, control, life-cycle management, and evaluation. This structured process provides a systematic method for agencies to minimize risks while maximizing the return on its IT investments.

We performed this audit to determine if the Department is effectively managing its Enterprise Architecture and ITIM efforts. The Department's IT budget for fiscal year (FY) 2005 is \$2.2 billion for 320 systems, including 22 major systems that cross-cut more than one organizational component of the Department. The Department continues to face significant challenges in ensuring that its IT systems are developed and deployed in a timely and cost-effective manner. For example, IT systems planning and utilization is one of the Department's top ten management challenges. Further, the management of the Department's IT investments has been a material weakness since FY 2002.

Congress enacted the Information Technology Management Reform Act of 1996 (known as the Clinger-Cohen Act) to address longstanding problems related to federal IT management. The Clinger-Cohen Act requires the head of each federal agency to implement a process that maximizes the value of agency IT investments and assesses and manages acquisition risks. A key goal of the Act is to ensure that agencies implement IT projects at acceptable costs and within reasonable timeframes. Under Clinger-Cohen, IT projects are to contribute to tangible and observable improvements in the mission performance of each agency. The act also requires the Chief

Information Officer (CIO) of each agency to develop, maintain, and facilitate the implementation of Enterprise Architectures as a means of integrating business processes with agency goals. The Office of Management and Budget (OMB) has also issued guidance on IT management (Circular A-130), which requires each federal agency to establish and maintain a capital planning and investment control process for IT.

The Department has not yet established an Enterprise Architecture or ITIM processes and therefore is not in compliance with the Clinger-Cohen Act, OMB guidance, and Department regulations. However, the Department is actively developing and implementing new frameworks aimed at establishing an Enterprise Architecture and ITIM processes. Also, some Department components, such as the Federal Bureau of Investigation (FBI) and the Drug Enforcement Administration (DEA), have made progress in developing component-level Enterprise Architectures and ITIM processes.

The Department's Justice Management Division, which manages the Department's cross-cutting systems and 20 of its own operational and administrative systems, began work in 1999 on developing an Enterprise Architecture and ITIM processes, but these efforts were overtaken by higher priority work on the broader Department-level Enterprise Architecture and ITIM processes. Previous attempts by the Department to develop an Enterprise Architecture and ITIM processes using established frameworks were troubled with false starts and a lack of focus and direction. The Department now anticipates that its current efforts to complete an Enterprise Architecture and fully implement ITIM processes will take several years. Without an established, comprehensive Enterprise Architecture and mature ITIM processes in place, the Department risks investing in IT systems that may be duplicative, poorly integrated, and costly to maintain.

## **Enterprise Architecture**

The Department's Enterprise Architecture efforts began in 1999. These efforts have suffered from a lack of institutional commitment and a changing perception of the composition and priority of a Department Enterprise Architecture. After several years spent attempting to develop an Enterprise Architecture using generally accepted frameworks, the Department decided to develop its own approach tailored to the Department's needs. Under a two-tiered approach, the Department's Justice Management Division (JMD) is responsible for developing Enterprise Architecture for the major IT systems that span multiple Department components, while component-specific IT systems will be covered by Enterprise Architectures developed by the respective Department

components. Together, these two levels of architectures will comprise a comprehensive Department Enterprise Architecture. JMD needs to oversee and coordinate the component-level Enterprise Architecture efforts to ensure they contribute to the formation of the Department's Enterprise Architecture. However, to date the Department has provided little oversight of the components' development of Enterprise Architectures.

JMD is developing a framework, called the Capability Delivery Model, to establish its Enterprise Architecture. The Department expects to complete the framework in late FY 2005 and the resulting Enterprise Architecture by late FY 2009. According to Department officials, the Capability Delivery Model will not be as high-level as the commonly used Federal Enterprise Architecture Framework (FEAF), but rather is intended to be more useful and relevant to day-to-day operations of the Department while containing the basic elements of the FEAF. The Department expects the Enterprise Architecture developed through the framework to cover the Department's major, cross-cutting IT systems and enable the Department to more effectively and efficiently manage its current and future IT infrastructure and applications. The Department estimated spending approximately \$1 million on Enterprise Architecture efforts in FY 2004 and predicts spending approximately \$1.1 million in FY 2005. However, Department officials were unable to provide us with specific expenditures related to the cost of Enterprise Architecture efforts from FY 1999 to 2004.

### GAO Framework

In April 2003, the U.S. Government Accountability Office (GAO), in collaboration with the OMB and the CIO Council, published an Enterprise Architecture framework.<sup>1</sup> The GAO framework provides measures to aid in assessing the progress of an organization's Enterprise Architecture efforts. The GAO framework describes five stages of Enterprise Architecture maturity and details the elements needed to achieve each stage.

Applying the GAO five-stage framework to assess what the Department has achieved toward developing its Enterprise Architecture, we found that the Department has completed six of the nine elements to reach a Stage 2 maturity level. The Department has adequate resources; a program office responsible for Enterprise Architecture development and maintenance; a Chief Architect; an Enterprise Architecture framework and methodology; plans for current, target, and transitional architectures in

---

<sup>1</sup> The framework is entitled *Information Technology, A Framework for Assessing and Improving Enterprise Architecture Management*, Version 1.1 (GAO-03-584G), dated April 2003.

terms of business, performance, information, application, and technology; and application of security within each architectural area. The Department does not have a Department-wide committee responsible for directing, overseeing, and approving the Enterprise Architecture; an automated tool; or metrics for measuring Enterprise Architecture progress, quality, compliance, and return on investment.

The Department has made progress toward attaining Stage 3 maturity. The Department has worked on developing a process for the establishment of current, target, and transition architectures. However, the Department lacks a written and approved policy for Enterprise Architecture development, implementation, and maintenance. In addition, the Department must ensure that when completed, all Enterprise Architecture products undergo configuration management.<sup>2</sup>

To attain Stage 4 maturity, the Department must complete additional work before the Enterprise Architecture can be used as intended — to drive sound IT investments that are consistent with the Department's goals and missions. The Department is working on a current architecture, transition plan, and target architecture, which it plans to complete by FY 2009.

To reach the Stage 5 level of a fully mature Enterprise Architecture, an organization must use its Enterprise Architecture to drive IT investments and ensure systems' interoperability. The Department cannot meet Stage 5 requirements of the Enterprise Architecture Management Framework until it completes its Enterprise Architecture.

The foundation of the Department's Enterprise Architecture lies in its IT infrastructure. A consolidated infrastructure will aid the Capability Architecture effort by providing a common conceptual framework to support technical interoperability, defining a common Department vocabulary, and providing a high-level description of the IT deployed throughout the Department. We found that the Department is developing the elements of a consolidated infrastructure through pilot programs.

Completion of a clear and comprehensive Department Enterprise Architecture will require a collaborative effort between the Department and the major Department components. The two-tiered architecture envisioned by the Department will require components to contribute Enterprise Architectures that encompass component-specific IT systems, which are not included in the Department's cross-cutting Capability Architectures.

---

<sup>2</sup> Configuration management is the process of managing changes to IT systems or hardware.

However, some components have been independently developing Enterprise Architectures for several years at considerable cost — \$26.7 million in FY 2004 — without substantive or consistent Department-level guidance or monitoring. While focusing on a Department-wide Enterprise Architecture methodology, the Department has not provided sufficient direction to ensure that components' Enterprise Architecture efforts are consistent with, and meet the needs of, the overall Department Enterprise Architecture. Also, the Department has not tracked the development of components' Enterprise Architectures, validated those Enterprise Architectures that have been developed, or ensured that Enterprise Architectures are kept current.

However, the Department has begun work to improve its oversight and guidance in this area. For example, an Enterprise Architecture Program Management Plan, completed June 2005, discusses the Department's Enterprise Architecture organization, interaction between the components and the Department, the need for a Department-wide Enterprise Architecture tool, and components' use of the FEAF.

### **Information Technology Investment Management**

A key objective of the Clinger-Cohen Act is to ensure that agencies implement processes for maximizing the value of IT investments and for assessing and managing the risks of IT acquisitions. To accomplish this objective, agencies must establish processes to ensure that IT projects are being implemented at acceptable costs and within reasonable timeframes, and that the projects are contributing to tangible, observable improvements in mission performance. Additionally, OMB Circular A-130 requires each federal agency to establish and maintain a capital planning and investment control process for IT. The Department is in the early stages of developing a Department-wide ITIM to share IT information, data, and infrastructure. Some Department components have developed or are developing their own ITIM processes, although the Department does not have overall information regarding the cost or status of these efforts.

Prior to FY 2004, the Department was not making investment decisions consistent with the development of a cohesive Department IT portfolio. Instead, the Department reviewed component IT concept proposals and budget requests to ensure alignment with the Department's 2002 IT Strategic Plan. In 2002, the Department initiated ITIM policies and procedures to comply with Clinger-Cohen but found the components were making slow progress in developing their ITIM processes. In October 2004, the Department issued a framework for developing ITIM processes, called the IT Strategic Management (ITSM) Framework. The Department expects

the ITSM Framework to lead to a Department-level ITIM and a high level of IT leadership and centralization of IT functions. The ITSM is intended to encompass all IT investments of the Department by providing direction to the larger components on what investment strategies to take, while also providing ITIM processes for smaller components where creating complete ITIM processes is impractical.

The Department's ITSM Framework consists of three phases: IT Planning, IT Funding and Architecture, and IT Investment Oversight.

- The IT Planning Phase establishes IT strategies and priorities for the Department through the development of an IT Strategic Plan and then builds on those strategies through the development of an IT Investment Plan.
- The IT Funding and Architecture Phase builds on the IT Planning Phase. The funding portion uses an IT Investment Plan to formulate a budget. This occurs while the architecture effort develops a "conceptual architecture" to guide project development by providing a standard for solution architectures. The primary product of the IT Funding and Architecture Phase is a funded enterprise portfolio.
- The IT Investment Oversight Phase monitors the progress of development and implementation of the Department's IT investments. This phase consists of a continuing evaluation of the Department's IT portfolio to determine whether investments should be made, existing systems should continue to operate, or systems should be eliminated.

With the implementation of the ITSM beginning in 2004, the Department's approach to IT management has begun to change from a decentralized to a more centralized approach. According to a Department official, the Department plans to take a more integrated approach and to focus more on IT management at the Department level. This new vision has resulted in a more proactive role by the Department in matching technology to identified business needs.

The ITSM framework is emphasizing the Department's oversight role to ensure that components' ITIM processes and investments are aligned with those of the Department. The Department's initial oversight of component ITIMs began in March 2001 with DOJ Order 2880.1A, which requires components to have an ITIM process. Initially the Department required components to submit their ITIM methodologies for review, but this oversight of components' ITIM processes was abandoned in 2002. After

2002, the Department changed its focus from the investment process to the investments and IT products themselves, and priorities became product-oriented instead of process-oriented. As a result of the ITSM, the Department is now refocusing on the investment process. However, the Department's current oversight effort centers almost exclusively on the FBI's ITIM, because the FBI's IT budget is the largest of the Department's components. While the Oversight Phase in the ITSM framework will be used to supervise components' IT projects, currently there is no Departmental oversight or approval of ITIM processes other than the FBI's.

## **Conclusions**

We found that although the Department is in the process of developing both an Enterprise Architecture and ITIM processes based on Department-developed frameworks, it is not yet in full compliance with the Clinger-Cohen Act, OMB guidance, or Department regulations. However, at this early stage of development, we believe the methodologies being implemented by the Department — the Capability Delivery Model for an Enterprise Architecture and the ITSM framework for ITIM — will comply with the requirements of Clinger-Cohen and OMB A-130, if brought to completion as planned. The Department has also begun to improve its oversight and guidance of the components' Enterprise Architectures and ITIM processes. However, additional oversight of the components is needed to ensure the success of the Capability Delivery Model and the ITSM framework.

## **OIG Recommendations**

In this report, we make seven recommendations for improving the Department's IT management. The recommendations are:

- Complete the Department-wide Enterprise Architecture to ensure that IT investments are not duplicative, are well-integrated, are cost-effective, and support the Department's mission.
- Provide Departmental guidance to components for the development and maintenance of Enterprise Architectures consistent with the guidance provided by the Federal Enterprise Architecture Framework, the OMB, and the GAO.
- Track and review the planning, development, completion, and updating of component-level Enterprise Architectures.



- Meet the requirements established by the Clinger-Cohen Act by fully implementing the phases outlined by the ITSM framework to ensure that all Department IT investments are covered by an ITIM process.
- Ensure that components requiring ITIM processes develop them.
- Provide assistance to components in developing and implementing ITIM processes.
- Establish a clear schedule for the completion of the ITSM framework and the completion of a mature ITIM process.

## TABLE OF CONTENTS

BACKGROUND .....	1
Introduction .....	1
Authorities .....	1
Departmental Guidance .....	3
Enterprise Architecture Management.....	5
IT Investment Management.....	9
Prior Reports .....	10
 FINDINGS AND RECOMMENDATIONS .....	 11
Finding 1: Enterprise Architecture.....	11
Department-level Enterprise Architecture Efforts .....	11
Status of the Department's Progress toward Completing the Five Stages of the GAO Enterprise Architecture Framework .....	14
Department IT Infrastructure.....	24
Oversight of Components' Enterprise Architecture Development.....	26
Conclusion .....	28
Recommendations.....	30
 Finding 2: Information Technology Investment Management .....	 31
Department-level ITIM .....	31
Conclusion .....	45
Recommendations.....	47
 STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS .....	 48
STATEMENT ON INTERNAL CONTROLS .....	50
APPENDIX 1: OBJECTIVE, SCOPE, AND METHODOLOGY.....	51
APPENDIX 2: DOJ and OCIO ORGANIZATION CHARTS.....	53
APPENDIX 3: ACRONYMS .....	55
APPENDIX 4: SUMMARY OF ENTERPRISE ARCHITECTURE MANAGEMENT FRAMEWORK'S MATURITY STAGES, CRITICAL SUCCESS ATTRIBUTES, AND CORE ELEMENTS .....	56
APPENDIX 5: SUMMARY OF GAO ITIM FRAMEWORK .....	57

APPENDIX 6: DEPARTMENT PROGRESS THROUGH STAGE 3 OF THE ENTERPRISE ARCHITECTURE MANAGEMENT FRAMEWORK.....	60
APPENDIX 7: THE THREE COMPONENTS OF THE ITIM PROCESS.....	62
APPENDIX 8: PRIOR REPORTS .....	64
APPENDIX 9: DEPARTMENT ITSM FRAMEWORK'S CONTINUOUS INTEGRATED PROCESSES.....	67
APPENDIX 10: THE DOJ'S RESPONSE TO THE DRAFT REPORT.....	69
APPENDIX 11: OFFICE OF THE INSPECTOR GENERAL'S ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT .....	73

## **BACKGROUND**

### **Introduction**

The Department of Justice (Department) relies on 320 Information Technology (IT) systems to conduct the business of the Department through its components, offices, boards, and divisions. Most of these IT systems are unique to the major organizational components of the Department, although 22 major systems cross-cut more than one component. In Fiscal Year (FY) 2005, the Department budgeted nearly \$2.25 billion for IT, and almost half the budget applied to cross-cutting systems.

### **Authorities**

#### Clinger-Cohen Act

Congress enacted the Information Technology Management Reform Act of 1996 (known as the Clinger-Cohen Act) to address longstanding problems related to federal IT management. The Clinger-Cohen Act requires the head of each federal agency to implement a process that maximizes the value of agency IT investments and assesses and manages acquisition risks. A key goal of the Act is to ensure that agencies implement IT projects at acceptable costs and within reasonable timeframes. Under Clinger-Cohen, IT projects are to contribute to tangible and observable improvements in the mission performance of each agency.

Clinger-Cohen also requires the Chief Information Officer (CIO) of each agency to develop, maintain, and facilitate the implementation of IT architectures as a means of integrating business processes with agency goals. An IT architecture, commonly referred to as an organization's Enterprise Architecture, is an integrated framework used to acquire, evolve, or maintain IT that achieves strategic and information resource management goals.

The Clinger-Cohen Act assigns to the head of an executive agency the responsibility to develop a capital planning and investment control process that will:

- provide for the selection, management, and evaluation of investments;
- be integrated with the budget, management, and program management processes;

- include minimum performance criteria for comparing and prioritizing alternative investment projects;
- identify investments that would result in shared benefits or costs for other agencies;
- identify quantifiable measurements for net benefits and risks of investments; and
- provide the means for senior management to obtain timely information regarding the progress of an investment.

### OMB Circular A-130

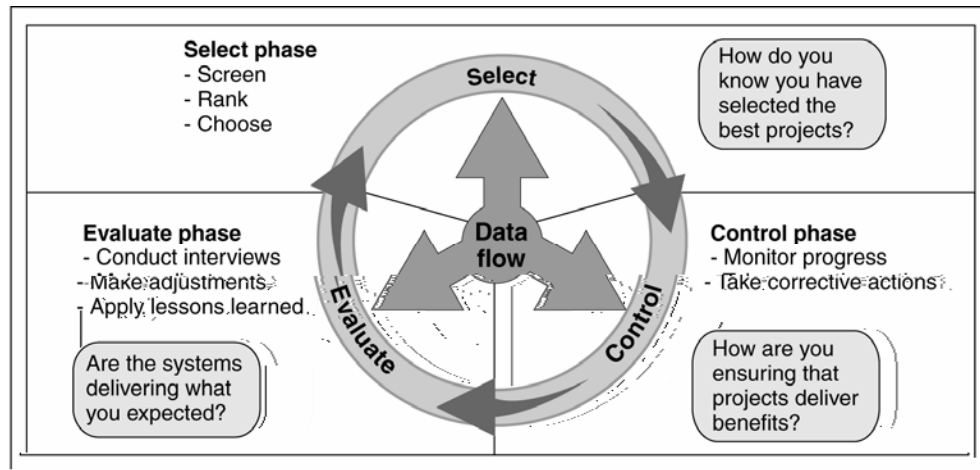
Office of Management and Budget (OMB) Circular A-130 (A-130) requires each federal agency to establish and maintain a capital planning and investment control process for IT, commonly referred to as Information Technology Investment Management (ITIM). The major purpose of establishing an ITIM process is to link agency resources with agency results. The ITIM process is intended to guide strategic and operational information resource management, IT planning, and the Enterprise Architecture. This is accomplished by integrating the agency's budget execution processes with statutorily required strategic and performance, financial management, and acquisition plans.<sup>3</sup>

According to OMB Circular A-130, agencies are to use an ITIM process to link mission needs, information, and IT in an effective and efficient manner. An effective ITIM process has three components: select, control, and evaluate. The following chart describes the three fundamental phases of this IT investment approach.

---

<sup>3</sup> Each agency prepares these plans pursuant to specific mandates. Agency strategic and performance plans are required by the Government Performance and Results Act of 1993, agency financial management plans are required by the Chief Financial Officer Act of 1990, and agency acquisition plans are required by the Federal Acquisition Streamlining Act of 1994.

## FUNDAMENTAL PHASES OF THE IT INVESTMENT APPROACH



Source: Government Accountability Office

A-130 also requires agencies to document and submit their initial Enterprise Architectures to the OMB, as well as updates when significant changes occur. The Enterprise Architecture is to describe both the current architecture of an agency and its future, or target, architecture, as well as provide a roadmap enabling the agency to both support its current IT state and transition to a targeted environment. Such roadmaps include an agency's capital planning and investment control processes, Enterprise Architecture planning processes, and system life cycle methodologies.

### Departmental Guidance

In order to meet the requirements of Clinger-Cohen and A-130, the Department issued guidance to its components in March 2001, which provided a framework for developing ITIM processes, including those covering Enterprise Architectures.

#### DOJ Information Resources Management Policy

In March 2001, the Department's Assistant Attorney General for Administration approved DOJ Order 2880.1A, Information Resources Management, which established an Information Resources Management (IRM) policy for the Department based on Clinger-Cohen. This IRM policy applies to all major Department components.

The order requires each component to designate a CIO to serve as the primary point of contact for IRM policy and requires the component CIO to: (1) report directly to the respective component head, and (2) recommend a

component-level ITIM process that both budgets for and prioritizes IT investment deployment. The component CIO is to submit the component's ITIM process to the DOJ CIO for approval upon completion. Once the process is approved by the DOJ CIO, the component is responsible for managing its respective IT investment portfolios and establishing component ITIM decision-making forums and policies. The order also requires the components to develop and maintain Enterprise Architectures to support their ITIM processes.

### DOJ ITIM Guide

In August 2001, the Department issued *The Guide to the Department of Justice Information Technology Investment Management Process (Guide)* to implement the Clinger-Cohen Act, OMB Circular A-130, and other IT management requirements.<sup>4</sup> The *Guide* requires all DOJ components to implement an ITIM model and provides structure and support to DOJ components developing an ITIM model tailored to the unique characteristics of each component. The elements of an adequate ITIM process, regardless of component size, mission, or operational requirements, are also included in the *Guide*. Using the select-control-evaluate methodology, the components are to establish a structured, repeatable, and documented process for IT investments throughout the life cycle of the investment.

The select-control-evaluate method outlined in the *Guide* is intended to maximize component resources by focusing on strategic investment planning decisions for ongoing and future budget requests. By integrating each component's existing strategic planning, budgeting, and decision-making processes, the component's ITIM is to conform with Departmental policies and guidance and include timely and substantive executive-level review at the component level.

The requirements established in the *Guide* apply to all IT projects and systems in the Department, and accordingly each Department component must:

- designate a CIO who reports directly to the head of the component as required by DOJ Order 2880.1A,

---

<sup>4</sup> The additional requirements include the Government Performance and Results Act, Government Paperwork Reduction Act, Federal Acquisition Streamlining Act, Federal Acquisition Reform Act, Executive Order 13011, OMB Circular A-11, and OMB Memorandum M-00-07.

- establish an Executive Review Board to approve the component's IT portfolio and provide management oversight of decisions made about specific IT investments contained within the IT portfolio, and
- establish a component ITIM process that is both consistent with Departmental guidance and customized to function within the unique environment of the component.

#### Technical Reference Model

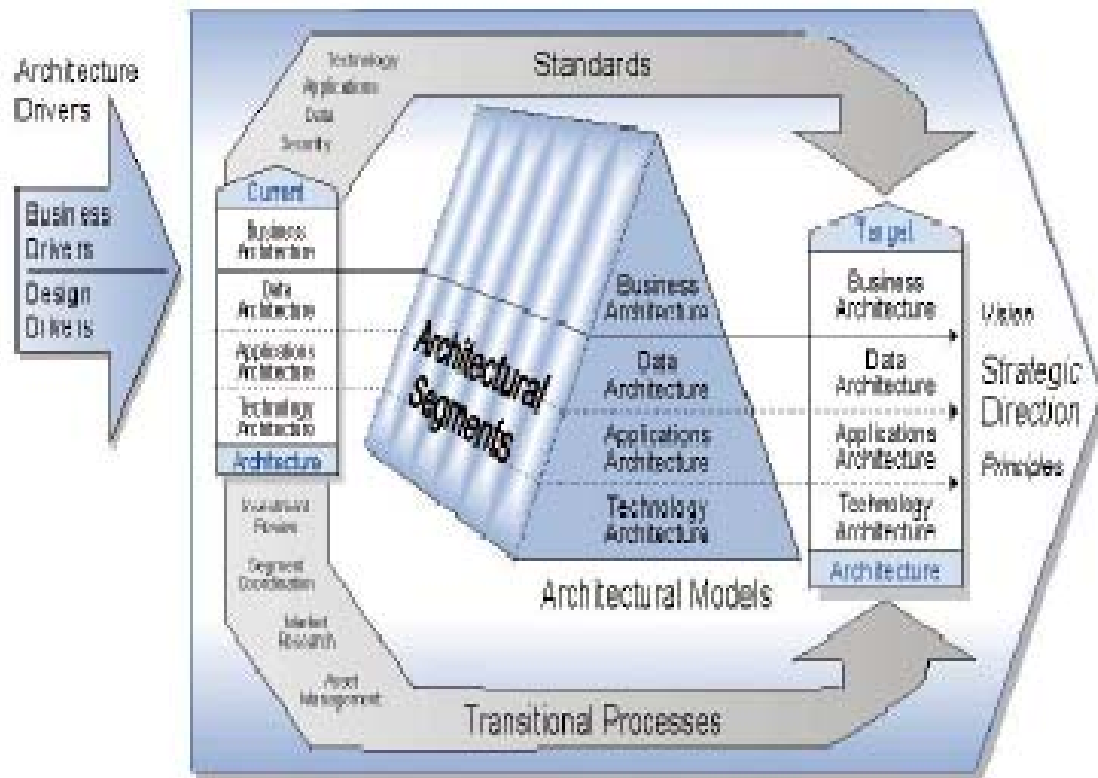
To facilitate the development of the Department's Enterprise Architecture, the Department issued a Technical Reference Model (TRM) in 2001. The TRM is not an architecture, but an aid to developing architectures for the Department. The TRM provides a foundation for developing technical and operational architectures, for defining services, and for identifying standards for all IT systems funded by the Department. It applies to both the development of new systems and the enhancement of existing systems. Use of the Department TRM was intended to promote the development and deployment of information systems that will enhance interoperability among components and their information systems.

#### **Enterprise Architecture Management**

In 1999, the Federal Chief Information Officers Council (CIO Council) issued the Federal Enterprise Architecture Framework (FEAF). This framework is illustrated in the following diagram.



## FEDERAL ENTERPRISE ARCHITECTURE FRAMEWORK



Source: Federal CIO Council

In support of the framework, the CIO Council issued the *Practical Guide to Federal Enterprise Architecture* (Practical Guide) in February 2001.<sup>5</sup> The Practical Guide describes Enterprise Architecture as a strategic information asset base that defines the mission, the technologies necessary to perform the mission, and the transitional processes for implementing new technologies in response to changing mission needs. An Enterprise Architecture is to provide a clear and comprehensive layout of an entity, whether the entity is an organization or a functional or mission area. According to the Government Accountability Office (GAO), investing in IT without defining the IT investments in the context of an Enterprise Architecture often results in systems that are duplicative, not well integrated, and costly to maintain.

<sup>5</sup> The CIO Council is the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of federal government agency information resources. The CIO Council's Practical Guide provides a step-by-step process to assist agencies in defining, maintaining, and implementing Enterprise Architectures.

An Enterprise Architecture is comprised of four elements: Business Architecture, Data Architecture, Applications Architecture, and Technology Architecture. Together, these elements provide a clear picture of how an organization accomplishes its mission, goals, and objectives. It also provides the baseline from which initiatives are planned and later compared.

Each of the four architectures is comprised of a current or “as-is” element that describes the existing environment, a target or “to-be” element that describes the proposed environment, and a sequencing plan detailing the transition from the “as-is” to the “to-be” environment.

In April 2003, the GAO, in collaboration with the OMB and the CIO Council, published an updated Enterprise Architecture management framework.<sup>6</sup> The GAO’s new Enterprise Architecture management framework provides measures to aid management in assessing its progress and taking any necessary corrective action. The GAO Enterprise Architecture framework consists of three basic components: (1) five hierarchical stages of management maturity, (2) categories of attributes that are critical to the success of managing any endeavor, and (3) elements of Enterprise Architecture management that form the core of the CIO Council’s *Practical Guide*.

The GAO framework outlines five maturity stages. These stages include steps toward achieving a stable and mature process that develops, maintains, and implements the Enterprise Architecture of an agency. As an organization improves its Enterprise Architecture management capabilities, its Enterprise Architecture management maturity subsequently increases. The five maturity stages are:

- **Stage 1: Creating Enterprise Architecture Awareness**  
A Stage 1 organization does not have plans to develop and use an architecture, or it has plans that do not demonstrate an awareness of the value of having and using an architecture. Efforts are ad hoc and unstructured, lack institutional leadership and direction, and do not provide the management foundation necessary for successful development.

---

<sup>6</sup> The framework is entitled *Information Technology, A Framework for Assessing and Improving Enterprise Architecture Management*, Version 1.1 (GAO-03-584G), dated April 2003.

- **Stage 2: Building the Management Foundation**  
A Stage 2 organization recognizes that an Enterprise Architecture is a corporate asset by vesting accountability in an executive body that represents the entire enterprise, assigning management roles and responsibilities, establishing plans for developing the Enterprise Architecture and for measuring program progress and quality, and committing the resources necessary for developing the architecture.
- **Stage 3: Developing the Enterprise Architecture**  
A Stage 3 organization focuses on developing architecture products according to the selected framework, methodology, and established management plans. The scope of the architecture has been defined to encompass the entire enterprise, whether organization-based or function-based. Products are intended to describe the organization in business, performance, data, application, and technology terms. Products are to describe the “as-is” and “to-be” states and the plan for transitioning from the current to the future state (the sequencing plan). The organization is tracking and measuring its progress against plans, identifying and addressing variances, and reporting on its progress.
- **Stage 4: Completing the Enterprise Architecture**  
A Stage 4 organization has completed its products and obtained the approval of a steering committee (or an investment review board) and the CIO. Evolution of the approved products is governed by a written maintenance policy approved by the head of the organization.
- **Stage 5: Leveraging the Enterprise Architecture to Manage Change**  
A Stage 5 organization has obtained senior leadership approval of products and has established a written institutional policy stating that IT investments must comply with the architecture, unless granted an explicit compliance waiver. Decision-makers are using the architecture to identify and resolve ongoing and proposed IT investments that are conflicting, overlapping, not strategically linked, or redundant. The organization tracks and measures benefits or return on investment, and adjustments are continuously made to the Enterprise Architecture management process and products.

With the exception of the first stage, each maturity stage is composed of the following four success attributes that are critical to the successful performance of any management function:

- **Demonstrates Commitment** by the head of the enterprise providing support and sponsorship to achieve the success of the Enterprise Architecture effort.
- **Provides the Capability to Meet Commitment** by developing, maintaining, and implementing Enterprise Architecture through adequate resources, clear definitions of roles and responsibilities, and implementing organizational structures and process management controls that promote accountability and effective project execution.
- **Demonstrates Satisfaction of Commitment** to develop, maintain, and implement Enterprise Architecture by producing Enterprise Architecture plans and products.
- **Verifies Satisfaction of Commitment** by measuring and disclosing the extent to which efforts to develop, maintain, and implement the Enterprise Architecture have fulfilled stated goals or commitments. Measuring performance allows for tracking progress toward stated goals, allows appropriate actions to be taken when performance deviates significantly from goals, and creates incentives to influence both institutional and individual behaviors.

Collectively, these attributes form the basis by which an organization can institutionalize the management of any given function or program, such as Enterprise Architecture management. Each attribute contains core elements that contribute to the effective implementation and institutionalization of a critical success attribute. Appendix 4 summarizes the interrelationships of the elements in the Enterprise Architecture management process.

## **IT Investment Management**

In 1997, the GAO issued *Assessing Risks and Returns: A Guide For Evaluating Federal Agencies' IT Investment Decision-making*, in which the GAO stated that investments in IT can have a dramatic impact on an agency's performance. Well-managed IT investments that are carefully selected and focused on meeting mission needs can propel an agency forward, dramatically improving performance while reducing costs.

Likewise, poor investments, those that are inadequately justified or whose costs, risks, and benefits are poorly managed, can hinder and even restrict an agency's performance.

To provide a method for evaluating and assessing how well an agency is selecting and managing its IT resources, in May 2000 the GAO issued *Information Technology Investment Management: A Framework For Assessing and Improving Process Maturity*, and updated the framework in March 2004. The GAO's ITIM framework outlines a set of essential and complementary management disciplines such as ITIM, strategic planning, and software development. The ITIM framework supports the fundamental requirements of the Clinger-Cohen Act and is intended to be used as a tool for implementing the required processes. Appendix 5 contains a summary of the GAO ITIM Framework.

OMB Circular A-130 requires that agencies establish and maintain a capital planning and investment control process that links mission needs, information, and information technology in an effective and efficient manner. A-130 divides the process into the Select, Control, and Evaluate stages. See Appendix 7 for summary of OMB Circular A-130's three ITIM stages.

## **Prior Reports**

We identified eight reports issued since May 2000 by the GAO and the Office of the Inspector General (OIG) that are relevant to this audit. See Appendix 8 for details of the eight reports.

In general, the GAO has reported that although almost all federal agencies had created some type of ITIM process, none had yet implemented stable processes addressing all three phases of the select-control-evaluate approach. The GAO also reported that the federal government as a whole had not reached a mature state of Enterprise Architecture management. The OIG reports identified vulnerabilities with management, operational, and technical controls in specific Department IT systems. In addition, the OIG examined the status of Federal Bureau of Investigation (FBI) and Drug Enforcement Administration's (DEA) ITIM processes and Enterprise Architectures.

## **FINDINGS AND RECOMMENDATIONS**

### **Finding 1: Enterprise Architecture**

The Department of Justice does not yet have an Enterprise Architecture despite intermittent efforts begun in 1999. However, the Department is developing and implementing frameworks aimed at establishing an Enterprise Architecture, which the Department expects to complete by 2009. When completed, the Enterprise Architecture should provide a blueprint for the Department to more effectively and efficiently manage its current and future IT infrastructure and applications. The Department abandoned its earlier attempts to develop an Enterprise Architecture using generally accepted frameworks and is now developing a Department-level Enterprise Architecture for the major cross-cutting IT systems that span multiple Department components, and component-specific IT systems that will have Enterprise Architectures developed by the respective components. However, we found that the Department is providing little oversight of the components' development of Enterprise Architectures. It is also unclear whether the Department's two-tier approach will result in an Enterprise Architecture that encompasses all IT throughout the Department. Without a comprehensive Enterprise Architecture, the Department risks investing in IT systems that could be duplicative, poorly integrated, and costly to maintain. The successful completion of the Department's Enterprise Architecture, along with individual components' Enterprise Architectures, will mitigate those risks and provide a realistic vision of future IT requirements.

#### **Department-level Enterprise Architecture Efforts**

Efforts to develop a Department Enterprise Architecture have been underway since 1999. However, the Department's efforts to develop an Enterprise Architecture have suffered from a lack of institutional commitment and a changing perception of the composition of, and priority for, a Department-level Enterprise Architecture. Adding to this confusion are the additional Enterprise Architectures developed by components.

In 2001, the Department began developing an Enterprise Architecture based on the Federal Enterprise Architecture Framework (FEAF). The Department secured funding and hired System, Data, Infrastructure, and

Business Architects and an Investment Management Coordinator. This group assembled “as-is” business, data, and application architectures by December 2001. However, a Department official told us that other priorities prevented this early Enterprise Architecture effort from continuing. Further, the “as-is” architectures were not updated and were not useful for later efforts to develop a Department-wide Enterprise Architecture.

In 2002, the Department began using the Federal Enterprise Architecture Management System (FEAMS), a web-based automated tool that provides agencies with access to initiatives aligned to the FEAF and associated reference models to assist in developing an Enterprise Architecture.<sup>7</sup> The FEAMS was designed in close cooperation with the OMB, and the OMB required the Department to use the FEAMS to develop its Enterprise Architecture. According to a Department official, the Department considered the FEAMS to be a cumbersome system that made inputting and extracting data difficult. Further, while the system served as a storage place for models, it could not perform analyses. Consequently, despite the OMB’s direction, the Department discontinued the FEAMS.

In 2003, the Department piloted the Popkin System Architect software for use as its automated tool. Although the DEA used the Popkin software in developing its Enterprise Architecture, a Department official stated that Popkin would require significant modifications to serve the Department’s purposes. Based on the results of the pilot, the Department decided not to use Popkin. A Department official stated that commercial off-the-shelf tools are now being explored as aids to the development of the Enterprise Architecture. However, the Department has no timetable for acquiring an automated tool to document the development of the Department’s Enterprise Architecture. In addition, Department officials were unable to provide expenditure data for Enterprise Architecture efforts prior to FY 2004.

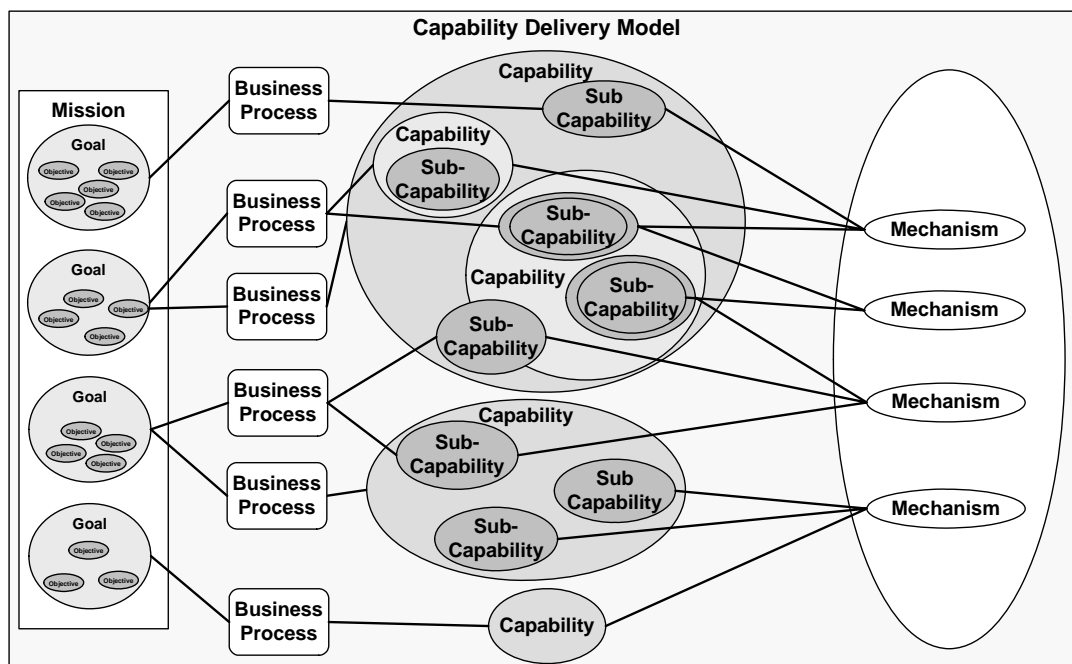
After rejecting the FEAF along with the FEAMS automated tool, the Department began devising its own framework intended to lead to a Department-wide Enterprise Architecture. The Department expects the framework, called the Capability Delivery Model, to be completed in late FY 2005 and the resulting Enterprise Architecture by late FY 2009. According to Department officials, the Capability Delivery Model, while including the basic elements of the FEAF, will not be as high-level as the FEAF, but rather is intended to be more useful and relevant to day-to-day operations. The Department expects the Enterprise Architecture developed through the Capability Delivery Model to cover the Department’s major,

---

<sup>7</sup> An automated tool is an electronic repository for capturing, updating, and disseminating an Enterprise Architecture across an organization.

cross-cutting IT systems and enable the Department to more effectively and efficiently manage its current and future IT infrastructure and applications.

The Department anticipates the Capability Delivery Model will be a more detailed, refined, Department-specific version of the FEAF. The foundation of the model is the Department's mission areas. For each mission area, component-specific goals and objectives will be developed, and capabilities will be identified to achieve them. Mechanisms — including systems, hardware, and software — will be obtained to support multiple capabilities. This process is illustrated in the following diagram.



Source: Justice Management Division

The Capability Delivery Model is being developed by creating several pilot architectures for categories of systems, such as an architecture for Terrorism Information Sharing, which stems from the Department's mission to prevent terrorism. A goal derived from this mission is the sharing of information among Department components involved in counterterrorism efforts. Examples of objectives within this goal are the interoperability, accessibility, and security of shared information. Once the goals and objectives are clarified, relevant component business processes are evaluated to develop a capability to meet them. In this example, the capability is the Intelligence Terrorism Information Sharing Environment. Specific IT mechanisms will then be put in place to enable the Terrorism Information Sharing Environment to be implemented.



The Department has developed Capability Architectures for Security, Public Key Infrastructure (PKI), and Telecommunications, and is currently developing the following Capability Architectures:

- Terrorism Information Sharing
- Arson and Explosives
- Law Enforcement Information Sharing
- Case Management
- Financial Management
- E-Government
- Integrated Wireless Network
- Other Classified functions

The Department expects to combine these Capability Architectures to form an overall Department-level Enterprise Architecture and then use it to manage the development of IT systems that cross-cut multiple Department components. This approach of using Capability Architectures is what makes the Department's Enterprise Architecture different from one created through the FEAF. The FEAF methodology relies on the development of various reference models that describe an organization's business, data necessary to conduct the business, applications to manage the data, and technology to support the applications. Instead of relying on various reference models, the Department's Enterprise Architecture will focus on the specific missions of the organization. Department managers told us that this approach provides a more specific and useful architecture tailored to the Department. While these two methodologies for developing Enterprise Architectures differ, Department officials stated that the elements required in the FEAF will be present in the Department's Enterprise Architecture.

### **Status of the Department's Progress Toward Completing the Five Stages of the GAO Enterprise Architecture Framework**

We used the criteria in the GAO's Enterprise Architecture framework to evaluate the Department's progress in developing a Department-wide Enterprise Architecture. To implement each of the five maturity stages of the GAO framework discussed below, the Department must complete four critical success attributes: (1) demonstrate commitment, (2) provide the capability to meet the commitment, (3) demonstrate satisfaction of commitment, and (4) verify satisfaction of commitment. Each attribute contains core elements that contribute to the effective implementation and institutionalization of the critical success attribute. Collectively, these attributes form the basis by which an organization can institutionalize management of any given function or program.

We found that the Department has nearly completed what equates to Stage 2 of the five-stage GAO framework and has made some progress toward the third stage of maturity.

### *Stage 1 — Completed*

In meeting the criteria for this stage, the Department created an awareness of the value of developing and using an Enterprise Architecture by providing the management foundation necessary for successful Enterprise Architecture development, as defined in Stage 2.

### *Stage 2 — Nearing Completion*

The Department has completed five of the nine core elements required by the GAO framework and has achieved one of the four critical attributes. To meet the criteria for this stage, the Department needs to: (1) ensure the existence of adequate resources; (2) establish Department-wide committees responsible for directing, overseeing, and approving the Enterprise Architecture; (3) develop the Enterprise Architecture using an automated tool; and (4) develop metrics for measuring Enterprise Architecture progress, quality, compliance, and return on investment.

#### Critical Attribute 1: Demonstrates Commitment

To complete the first critical attribute for Stage 2 of the GAO framework, the Department must demonstrate its commitment to building an Enterprise Architecture management foundation by establishing two core elements:

- (1) ensure the existence of adequate resources; and
- (2) establish Department-wide committees responsible for directing, overseeing, and approving the Enterprise Architecture.

We determined the Department has not fully implemented the two core elements under the first critical attribute for Stage 2.

*Adequate Resources.* Obtaining adequate resources includes: (1) identifying and securing the funding necessary to support Enterprise Architecture activities; (2) hiring and retaining employees with the proper knowledge, skills, and abilities to plan and execute the Enterprise Architecture program; and (3) selecting and acquiring the tools and technology to support Enterprise Architecture activities.

According to a Department official, the Department spent approximately \$1 million on developing its Enterprise Architecture in FY 2004 and plans to spend approximately \$1.1 million in FY 2005, amounts that appear adequate for continuing development at this point. The Enterprise Architecture Program Management Office includes the Chief Architect, Enterprise Architecture Program Manager, Business Architect, Systems Architect, Data Architect, Infrastructure Architect, Security Architect, Configuration Manager, Senior Systems Architecture Consultant, and Technical Writer. In our opinion, these employees have sufficient knowledge and experience to establish an Enterprise Architecture.

However, the Department does not yet have a tool to assist in the development of its Enterprise Architecture that clearly and completely documents the Department's Enterprise Architecture. As discussed previously, the Department tested the Popkin System Architect tool and found it unacceptable. The Department is in the process of identifying tools and technology to support its Enterprise Architecture activities. Because the Department does not have all the adequate resources for an Enterprise Architecture, the first core element is not fully implemented.

*Enterprise Architecture Governing Committees.* Responsibility for directing, overseeing, and approving architectures should be given to a committee or group with cross-representation from throughout the enterprise. Establishing agency-wide responsibility and accountability is important to demonstrate the agency's commitment to building a management foundation for the Enterprise Architecture and obtaining buy-in from across the agency. Accordingly, the committee or group should include executive-level representatives from each line of the business, and these executive representatives should have the authority to commit resources and enforce decisions within their respective organizational units.

The Department had established an Enterprise Architecture Committee (EAC) in 2001, which reported to the Department of Justice CIO Council. However, the EAC is no longer active.<sup>8</sup> The EAC was established to support the formulation and adoption of a Departmental Enterprise Architecture by ensuring that the Department-level Enterprise Architecture met all federal requirements. Further, the EAC was a deliberative body for the Department's chief IT architects to:

---

<sup>8</sup> The Department CIO established the Council to support the implementation of the Clinger-Cohen Act and other federal laws and policies related to IT management. Among other things, the Council reviews and makes recommendations to the Department CIO on IT projects, strategies, policies, and procedures and practices — both Department-wide or for any component.

- provide a forum for sharing and discussing Enterprise Architecture information;
- coordinate activities related to Departmental and federal Enterprise Architecture issues and priorities;
- collaborate on Departmental Enterprise Architecture strategies, management issues, and policies and practices;
- make recommendations to the Council for appropriate action;
- foster networking among Departmental IT architecture professionals;
- promote technology and security awareness to enhance Enterprise Architecture planning;
- work together on cross-cutting issues to reduce redundant efforts and improve architectural consistency; and
- support an effective working relationship between the components and the Department's Justice Management Division (JMD) so that their respective Enterprise Architecture responsibilities can be met.

In our judgment, the membership of the EAC demonstrated an agency-wide leadership commitment to the Enterprise Architecture process. The EAC was comprised of the Chief Architects from the Federal Bureau of Prisons; DEA; FBI; Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Office of Justice Programs; Executive Office for U.S. Attorneys; JMD; U.S. Marshals Service; and other key architects within the Department. Also, a component CIO was designated to serve as EAC Chair, and the Department's Chief Architect was designated vice-chair.

The Committee met monthly from 2001 to 2002, then intermittently until disbanding in early 2004. Although a Department official stated the committee planned in early 2004 to regroup and begin meeting again, the Committee has been inactive since early 2004. The official explained that the Committee stopped meeting to rethink, regroup, and decide where the Department-wide Enterprise Architecture efforts were going. Therefore, the Department no longer meets one of the core elements required under the GAO framework to demonstrate its commitment.

## Critical Attribute 2: Provides Capability to Meet Commitment

The completion of the second critical attribute for achieving Stage 2 requires the Department to establish three core elements:

- (1) establish a program office responsible for Enterprise Architecture development and maintenance;
- (2) appoint a Chief Architect; and
- (3) develop the Enterprise Architecture using a framework, methodology, and automated tool.

The Department has made progress toward implementing these three core elements. The Department has implemented core elements 1 and 2, but core element 3 is not fully implemented.

*Enterprise Architecture Program Office.* Enterprise Architecture development and maintenance should be managed as a formal program. Accordingly, responsibility for Enterprise Architecture management should be assigned to an organizational unit and not an individual. The *CIO Practical Guide*, discussed in the Background section of this report, states that the primary responsibility of the Enterprise Architecture Program Office is to ensure the success of the Enterprise Architecture program.

Within the Department, JMD's Policy and Planning staff is responsible for maintaining, refining, updating, and applying the Department Enterprise Architecture. To implement this core element, the Policy and Planning staff gathers and maintains information about the Department's current state of IT resources and a "to be" target state. The target state aims to improve the current state in ways such as minimizing redundancy of IT services, improving the ability to share information Department-wide and with external stakeholders, and retiring IT assets that are no longer providing optimum service. Enterprise Architecture information, tightly coupled with cost information on IT business investments, helps the CIO make strategic decisions about the direction and evolution of the Department's IT services.

*Chief Architect.* The *CIO Practical Guide* and the GAO framework state that an agency should appoint a Chief Architect who is responsible and accountable for the Enterprise Architecture and whose background and qualifications include both the business and technology areas of the organization. Additionally, the Chief Architect is responsible for ensuring the

integrity of the Enterprise Architecture development process and for the content of the Enterprise Architecture products.

The Department has a Chief Architect who is the principal advisor to the Department's Chief Technology Officer and CIO on all Department-wide Enterprise Architecture matters. The Department's Chief Architect is responsible for:

- leading the development of Enterprise Architecture products,
- serving as the technology and business leader in ensuring the integrity of architectural development processes and products,
- providing technical and strategic planning and policy development, and
- providing guidance to capital planning and IT investments.

*Framework, Methodology, and Automated Tool.* The Department is developing its own Enterprise Architecture framework and methodology through its Capability Delivery Model. The Department's framework is to be an architecture based on capability areas within the entire Department and its components, with individual capability architectures acting as building blocks that are intended to form a Department-wide Enterprise Architecture. This Department-wide Enterprise Architecture will include both cross-cutting and component-specific capabilities.

An Enterprise Architecture automated tool serves as the storehouse of the architecture products. Architecture products include the current and target architectures and the transition plan. The choice of tool is based on the agency's needs and the size and complexity of the architecture. As stated previously, the Department tested the Popkin automated tool to store its architecture products but is now exploring alternatives to Popkin.

### Critical Attribute 3: Demonstrates Satisfaction of Commitment

The completion of the third critical attribute for achieving Stage 2 requires the Department to establish an Enterprise Architecture Program Plan that includes the following core elements:

- (1) describes both the current and the target architectures as well as a transition plan;

- (2) describes the current and target architectures in terms of business, performance, information, application, and technology; and
- (3) determines the application of security within each architectural area.

The Department's Enterprise Architecture Completion and Use Plan completes the three core elements under Critical Attribute 3.

*Current and Target Architectures, and Transition Plan.* The interagency CIO Council requires that agencies have a written Enterprise Architecture Program Plan. The plan should describe the steps to be taken and the tasks to be performed in managing the Enterprise Architecture program. The plan should also make provision for the development of architectural descriptions of how the organization currently operates (the current architecture), how it intends to operate in the future (the target architecture), and how it will transition from the current to the target environment (the transition plan).

The Department submitted a Department Enterprise Architecture Completion and Use Plan to the OMB in February 2005, and is working on a Department Enterprise Architecture Program Management Plan. The Department's Management Plan will:

- establish a Department-wide "as-is" architecture;
- update a capability-based target "to-be" architecture; and
- develop a transition or sequencing plan based on the Department-wide "to-be" architecture.

*Security.* The Department has a comprehensive Security Architecture in place that will be aligned with security standards for the Department's overall Enterprise Architecture efforts.

#### Critical Attribute 4: Verifies Satisfaction of Commitment

The completion of the fourth critical attribute to achieve Stage 2 requires the Department to ensure that the Program Plan calls for developing metrics for measuring Enterprise Architecture progress, quality, compliance, and return on investment. The Department has not implemented this core element.

The measurement of Enterprise Architecture progress, quality, and compliance is necessary to ensure that the Enterprise Architecture meets the targeted milestones and is compliant with necessary regulations. Measuring return on investment would tell the Department what benefits are realized by the development of the Enterprise Architecture in relation to its cost.

*Developing Metrics for Measuring Enterprise Architecture Progress.* The Department has not yet established metrics for measuring Enterprise Architecture progress, quality, compliance, and return on investment. The Department's Enterprise Architecture Completion and Use Plan states that Enterprise Architecture links performance measures to some portions of the architecture segments. This does not meet the criteria for the fourth attribute.

### *Stage 3 — Limited Progress*

The Department is moving from building the Enterprise Architecture management foundation to developing Enterprise Architecture products for Stage 3. To complete Stage 3, the Department must still: (1) establish an organization policy for the Enterprise Architecture development; (2) ensure that Enterprise Architecture products are under configuration management; (3) ensure that Enterprise Architecture products describe both the current and target environments of the agency; (4) ensure that the business, data, application, and technology descriptions address security; and (5) ensure that progress against Enterprise Architecture plans is measured and reported.

The Department has made limited progress toward attaining Stage 3 maturity of the GAO Enterprise Architecture Management Framework. The Department has made progress on developing a process for developing current, target, and transition architectures. However, the Department lacks a written and approved policy for Enterprise Architecture development, implementation, and maintenance. In addition, the Department must ensure that when completed, all Enterprise Architecture products undergo configuration management and that the Enterprise Architecture addresses security, as stated in the Enterprise Architecture Completion and Use Plan.

### Critical Attribute 1: Demonstrate Commitment

To complete the first critical attribute for Stage 3 of the Enterprise Architecture Management Framework, the Department must establish the following core element: develop a written and approved organization policy



for the Enterprise Architecture development. The Department has not completed this core element.

According to the Enterprise Architecture Management Framework, an organization policy is an important means for ensuring agency-wide commitment to developing the Enterprise Architecture and for clearly assigning responsibility for doing so. The architecture policy should define the scope of the architecture, including a description of the current and target architecture, as well as a transition plan that supports the move from the current to the target architecture. Additionally, the policy should provide processes for Enterprise Architecture oversight and control, review, and validation. The policy should also address the purpose and value of an Enterprise Architecture, its relationship to the organization's strategic vision and plans, and its relationship to the capital planning process.

The Department has not established a written and approved organization policy for Enterprise Architecture development. As described in Stage 2, the Department established the Enterprise Architecture Program Office with responsibility for developing the Enterprise Architecture. In addition, the Enterprise Architecture Program Management Plan — discussed in Stage 2 — outlines a high-level scope of the architecture, including a description of the planned current and target architecture, as well as the transition plan. The Enterprise Architecture Program Management Plan also addresses Enterprise Architecture oversight, control, review, and validation responsibilities, but in little detail.

#### Critical Attribute 2: Provides Capability to Meet Commitment

The completion of the second critical attribute for achieving Stage 3 maturity requires the Department to establish the following core element: ensure that Enterprise Architecture products are under configuration management.<sup>9</sup> The Department has not yet met this standard.

According to the draft of the Department Enterprise Architecture Program Management Plan, the Enterprise Architecture Program Office will perform configuration management of Enterprise Architecture Products. The Office will also prepare and publish policy to include establishment of necessary configuration committees.

---

<sup>9</sup> Configuration management is the process of managing changes to IT systems or hardware.

### Critical Attribute 3: Demonstrates Satisfaction of Commitment

The completion of the third critical attribute for achieving Stage 3 maturity requires the Department to establish three core elements:

- (1) ensure that Enterprise Architecture products describe the current and target agency environments and the transition plan;
- (2) ensure that the current and target environments are described in terms of business, data, application, and technology; and
- (3) ensure that the business, data, application, and technology descriptions address, or will address, security.

The Department has not implemented core elements 1 and 2. The Department addresses security in its Enterprise Architecture plans; therefore, core element 3 is complete.

*Current and Target Architectures, and Transition Plan.* According to the Enterprise Architecture Program Management Plan, Enterprise Architecture products will describe the current and target agency environments, as well as the transition plan. As stated earlier, the Department has not completed all components of the Enterprise Architecture. The current, target, and transition processes for the Department are to be identified, approved, and documented by the end of FY 2006. The Enterprise Architecture Program Plan also states that Enterprise Architecture products — current and target architectures and the transition plan — will be described in terms of business, data, application, and technology.

*Security.* The Department Enterprise Architecture Completion and Use Plan states that Enterprise Architecture will align security standards to the Technical Reference Model.

### Critical Attribute 4: Verifies Satisfaction of Commitment

The completion of the fourth critical attribute to achieve Stage 3 maturity requires the Department to establish the following core element: ensure that progress against Enterprise Architecture plans is measured and reported. The Department has not implemented this core element.

As stated in Stage 2, the Department has not established metrics for measuring Enterprise Architecture progress. The measurement of such

progress against Enterprise Architecture development plans is necessary to ensure that the development meets targeted milestones.

*Stage 4 — to be Completed*

Additional work must be completed before the Enterprise Architecture is used as intended in Stage 4 — to drive sound IT investments that are consistent with the Department's goals and missions.

To complete Stage 4, an agency

Currently, the Department's infrastructure is largely decentralized, fragmented and outdated. It is essentially an amalgamation of infrastructures designed, developed and maintained by individual components to meet their specific needs. This approach has introduced an unnecessary level of complexity, cost and risk, and inadvertently created technical barriers to sharing information.

The IT Strategic Plan establishes a Strategic Initiative to "develop the Infrastructure architecture layer of the Department's Enterprise Architecture." Specifically, "The Department will work with the components to develop a Department-wide infrastructure architecture — a layer of the Department's overall Enterprise Architecture. The infrastructure architecture will provide a common conceptual framework to support technical interoperability, define a common DOJ vocabulary, and provide a high-level description of the information technology deployed throughout the Department."

A consolidated infrastructure will aid the Capability Architecture effort. The Department is developing the elements of a consolidated infrastructure through a number of pilot programs. One example is the Public Key Infrastructure (PKI), created to resolve the Department's computer security concerns. PKI is intended to implement an IT security program as well as complete the design, development, and implementation of a secure and trusted IT environment.

The Infrastructure Architect is the person responsible for consolidating the Department's IT infrastructure. The Infrastructure Architect has described the following four critical elements of a consolidated infrastructure.

- Ubiquitous Communication: single, Department-wide communications application.
- Uniform Security: Department-wide security architecture and standards.
- Identity: identification of users and management with access to Department systems.
- Directory Service: Department-wide user database.

The Infrastructure Architect foresees cost savings, economies of scale in IT acquisitions, and enhanced enforcement of security and management of IT performance as benefits resulting from this consolidation. At the time of our field work, a draft Consolidated Infrastructure plan was nearing completion.

### **Oversight of Components' Enterprise Architecture Development**

Completion of a clear and comprehensive Department Enterprise Architecture will require a collaborative effort between the Department and the major Department components. The two-tiered architecture envisioned by the Department will require components to contribute Enterprise Architectures that encompass those component-specific IT systems that are not included in the Department's cross-cutting Capability Architectures. Some components, such as the FBI and the DEA, have made progress in developing their component-level Enterprise Architectures. Others, such as JMD, have not. In JMD's case, efforts begun in 2003 to develop a component-level Enterprise Architecture were held in abeyance as work began on the higher-priority Department-level Enterprise Architecture.

The Department's FY 2004 Report on Information Technology identifies funds budgeted for Enterprise Architecture and related planning. The table provides a 1-year snapshot of money budgeted for Enterprise Architecture efforts.

### **FY 2004 Component Enterprise Architecture (EA) Budgets**

<b>Component</b>	<b>Budget Line Item</b>	<b>Total Investment</b>
Bureau of Alcohol, Tobacco, Firearms and Explosives	EA/Configuration Management	\$3,900,000
Antitrust Division	EA/IT/IRM	\$1,065,000
Federal Bureau of Prisons	IRM	\$928,000
Community Oriented Policing Services	IT Architecture	\$475,000
Drug Enforcement Administration	EA/ITIM/Capability Maturity Model	\$1,204,000
Federal Bureau of Investigation	EA/ITIM	\$2,786,000
Interpol	IT Architecture/Planning	\$175,000
Justice Management Division	JMD/IMSS Architecture Program	\$1,521,000
National Drug Intelligence Center	EA/ITIM/IRM	\$940,000
Office of the Inspector General	EA and Planning	\$100,000
Office of Justice Programs	IT Management/Architecture	\$2,700,000
US Attorneys	IT Program Management	\$602,000
US Marshals Service	IT Management	\$10,317,000
<b>Total</b>		<b>\$26,713,000</b>

Source: Department of Justice FY 2004 Budget

In 2001, the Department requested that components submit their ITIM processes for review. However, the Department did not make a similar request for Enterprise Architectures. The Department also issued guidance, based on a Technical Reference Model, to develop a high-level Enterprise Architecture for the Department. A Department official stated that the only guidance provided to the components on Enterprise Architecture was through the Technical Reference Model and the Enterprise Architecture Committee (discussed in the Department Enterprise Architecture section of this report). Also, the Department did not track the development of components' Enterprise Architectures, validate Enterprise Architectures developed, or ensure that Enterprise Architectures were kept current.

According to the CIO, the Department conducts little oversight of component Enterprise Architectures. The CIO described a “broad brush” programmatic approach to the oversight of component Enterprise Architectures, which includes establishing standards and Enterprise Architecture tools, developing work plans for a Department-wide Enterprise Architecture, and establishing management of component-level Enterprise Architectures. However, as of June 2005, none of these efforts had been completed. At the same time, according to the CIO, the Department takes a “deep dive” approach in overseeing the components with selected Enterprise Architecture capability areas. According to the Chief Technology Officer (CTO), as discussed earlier the capability areas cross-cut multiple components and include Financial Management, Law Enforcement Information Sharing, Case Management, and the Justice Consolidated Office Network (JCON). The CTO also said there are several E-government-related architecture efforts in progress at the federal level for which the Department is either the managing partner or is an active participant. Therefore, these select few architectures merit more intensive Department oversight.

The CTO stated that components should develop project-specific architectures as necessary for projects that are a priority to the component, because these projects may not be included in the Department Enterprise Architecture. For architecture projects currently identified as common solutions or E-government projects, the Department Enterprise Architecture will provide guidance to the Enterprise Architecture program teams as necessary. The CTO stated that even though the Department is already informally involved to varying degrees with some components’ architecture efforts, it is in the process of establishing a formal Department Enterprise Architecture governance structure. The Department Enterprise Architecture program document will provide guidance to the components and program managers of other cross-component architecture efforts at the same time. According to the CIO, some of the common solution projects are underway and need a lesser degree of involvement from the Department’s Enterprise Architecture team. For architecture efforts that are identified as common, multi-component solutions in the future, the Department Enterprise Architecture will take the lead in developing the Enterprise Architecture teams and play a greater role in developing the architecture. All architecture efforts within the Department are to map their Enterprise Architecture to meet OMB, FEAF, and GAO guidance.

## **Conclusion**

An organization without a completed Enterprise Architecture assumes the risk that it will invest in IT that is duplicative, not well integrated, costly,

or not supportive of the agency's mission. Until a Department-wide Enterprise Architecture is completed, the Department faces such risks. Once the Enterprise Architecture is completed, the risks will be reduced and the Department will have a more realistic vision of its future IT requirements.

The current effort to develop a Department-wide, capability-based Enterprise Architecture for systems that cross-cut two or more components is in an early stage. Instead of being based on the generally accepted FEAF, this Enterprise Architecture will be based on the Department's self-created framework: the Capability Delivery Model. We believe it is too soon in the development of the model to determine if it will contain all the necessary elements of an Enterprise Architecture. It is also too soon to determine if, when fully developed, the model will result in an Enterprise Architecture that conforms to GAO, FEAF, and OMB guidance.

The Department believes that the most efficient approach to its Enterprise Architecture is to focus its efforts on major, cross-cutting IT systems with individual architectures for groups of systems such as case management systems. Component-level projects are expected to be covered by component-level Enterprise Architectures, which together with the Capability Architectures are to form the Department Enterprise Architecture. The Capability Delivery Model approach focuses on the high-visibility and high-cost cross-cutting IT projects. We believe that focusing management attention on high-risk projects is a prudent approach. However, a successful Enterprise Architecture should present a clear and comprehensive view of an organization, and the Department must take care to avoid a disjointed, fragmented, or incomplete Enterprise Architecture. Our audit found a lack of consistent coordination between the Department and component Enterprise Architecture efforts, which increases the risk that the Department's two-tiered approach could result in gaps within the Department's Enterprise Architecture.

In the course of conducting this audit, and in reviewing previous audits of DEA and FBI IT management, we found that the Department's oversight of component Enterprise Architecture efforts in general continues to be inconsistent. Components have been developing Enterprise Architectures for several years at considerable cost without ongoing and substantive Department-level guidance or monitoring. The Department is not currently providing direction to ensure that components' Enterprise Architecture efforts are consistent with, and will meet the needs of, the overall Department Enterprise Architecture under development. The Department's two-tiered approach to Enterprise Architecture will require all major components responsible for IT systems to develop Enterprise Architectures



in order for the overall Department Architecture to present a clear and comprehensive view of the Department's IT environment. However, the components have generally been working on their Enterprise Architectures independently, without specific guidance or monitoring to ensure full compatibility with the Department-level Enterprise Architecture when it is developed.

The Department has begun to improve its oversight and guidance of components' Enterprise Architecture efforts. For example, an Enterprise Architecture Program Management Plan, completed in June 2005, discusses the Department's Enterprise Architecture organization, interaction between the components and the Department, the need for a Department-wide Enterprise Architecture tool, and components' use of the FEAF. However, more progress is needed, and we provide the following recommendations for the Department.

### **Recommendations:**

We recommend that JMD:

1. Complete the Department-wide Enterprise Architecture to ensure that IT investments are not duplicative, are well-integrated, are cost-effective, and support the Department's mission.
2. Provide Departmental guidance to components for the development and maintenance of Enterprise Architectures consistent with the guidance provided by the FEAF, the OMB, and the GAO.
3. Track and review the planning, development, completion, and updating of component-level Enterprise Architectures.

## **Finding 2: Information Technology Investment Management**

The Department of Justice is in the early stages of developing the ITIM processes required by the Clinger-Cohen Act. These processes include selecting, evaluating, and managing IT investments while ensuring that agency missions are being supported. The Department's initial efforts to comply with Clinger-Cohen began in 2001, but progress has been limited. In 2004, the Department developed an Information Technology Strategic Management (ITSM) Framework that should enable the Department to implement Department-level ITIM processes and properly oversee the components' efforts. The Department expects its ITSM framework to lead to high-level IT leadership and centralization of IT functions, guide components that need assistance in implementing their own ITIM processes, and provide ITIM processes for smaller components that do not yet have them. The ITSM framework is also intended to result in integrating the components' ITIM processes with the Department's high-level ITIM processes. To fully comply with Clinger-Cohen, however, the Department must ensure that all IT investments follow effective selection, evaluation, and management practices. Due to the early stages and fragmented nature of the Department's overall ITIM development, the Department risks making IT investments that are duplicative or that do not fully support the agency's mission. Such risks will be greatly mitigated once the Department and its components establish and follow mature ITIM processes.

### **Department-level ITIM**

A key objective of the Clinger-Cohen Act is to ensure that agencies implement processes for maximizing the value of IT investments and for assessing and managing the risks of IT acquisitions. To accomplish this objective, agencies must establish processes to ensure that IT projects are being implemented at acceptable costs and within reasonable timeframes, and that the projects are contributing to tangible, observable improvements in mission performance. Additionally, OMB Circular A-130 requires each federal agency to establish and maintain a capital planning and investment control process for IT. The Department is in the early stages of developing Department-wide ITIM processes.

The Department and its components made various attempts to develop ITIM policies and procedures under Clinger-Cohen beginning in

2001, but progress has been slow. In October 2004, the Department issued a framework for developing ITIM processes, called IT Strategic Management (ITSM). The purpose of the ITSM framework is to:

- consolidate the processes of IT policy and planning into a coordinated IT planning and management effort;
- serve as a communication vehicle for delineating the relationships between Departmental and component IT planning and management activities;
- define products for which guidance and performance measures can be developed; and
- provide a context for building tactical project plans to operate IT selection, evaluation, and management.

Once the processes created through the ITSM framework are fully developed, the Department expects that the components' ITIM processes and functions will be integrated within the Department's overall ITIM structure. The Department-level ITIM will then support all components regardless of size, funding, or resources. In order to achieve this objective and ensure coverage of all IT projects within the Department, components that have or are developing ITIM processes will be required to incorporate the Department's ITSM framework into their own frameworks.

The following tables summarize Clinger-Cohen and OMB A-130 requirements and how the ITSM framework is to meet them.

<b>Clinger-Cohen Requirements</b>	<b>ITSM Framework Characteristics</b>
Provide for selection, management, and evaluation of investments.	A framework that aligns with the OMB Investment Management Process Model for the selection, control, and evaluation of investments. <sup>10</sup>
Integrate with budget, financial, and program management processes.	An IT Funding and Architecture Phase that integrates OMB IT submissions with the Department budget processes.
Include minimum performance criteria for comparing and prioritizing alternative investment projects.	An IT Strategic Planning Phase that considers strategic alternatives, technical alternatives, and investment alternatives.
Identify investments with shared benefits of costs for other agencies.	An Investment Planning Process for Enterprise Architecture that develops Enterprise Architecture with Federal partners to provide optimal solutions.
Identify quantifiable measurements for net benefits and risks of the investment.	Performance measures to be developed for investments.
Provide the means for senior management to obtain timely information regarding the progress of an investment.	An Investment Oversight Phase with tools and mechanisms to review processes for reporting timely information to senior management.

Source: Department ITSM Framework

---

<sup>10</sup> The OMB Investment Management Process Model establishes an analytical framework for linking IT investment decisions to strategic objectives and business plans in federal organizations. Federal organizations are to use this model in developing their own ITIM frameworks.

OMB Circular A-130 Requirements	ITSM Framework Characteristics
Monitor investments.	An IT Oversight Phase for monitoring investments, and a web-based Dashboard to summarize the status of investments. (The Dashboard is discussed later in this report.)
Prevent redundancy of existing or shared IT capabilities.	A Strategic Planning Process that analyzes the Department's capability needs and develops strategies for meeting these needs, using non-redundant technologies.
Demonstrate the impact of alternative IT investment strategies and funding levels.	<p>An Investment Planning Process that considers alternative technical and resource strategies.</p> <p>An IT Funding and Architecture Phase that works in conjunction with the Budget Process to optimize funding levels.</p>
Identify opportunities for sharing resources and consider their inventory of information as resources.	An Investment Planning Process for Enterprise Architecture and Human Capital, which includes the development of transition strategies for optimizing technical Departmental assets and human capital.

Source: Department ITSM Framework

To assist organizations with developing ITIM processes, the GAO developed *ITIM: A Framework for Assessing and Improving Process Maturity*, which provides a method for evaluating how well an agency is selecting and managing its IT resources. This framework is built around the select/control/evaluate approach described in Clinger-Cohen. The most current version, issued in 2004, is a maturity model composed of five

progressive stages.<sup>11</sup> Appendix 4 outlines the GAO framework. We intended to use the GAO ITIM framework to evaluate the status of the Department's ITIM but did not do so because of the Department's limited progress in establishing its ITIM processes. Instead, we examined the Department's ITSM framework to determine whether it would allow for the development of effective ITIM processes.

Since 2002, the Department has worked on various policies and procedures related to developing a Department-wide ITIM. In addition to the Department's ITSM framework, the Department created a web-based "Dashboard" tool to show IT investment information and status, an IT Strategic Plan to set IT strategic goals, and a Department Executive Review Board (DERB) Charter to provide oversight for components' IT investments. A discussion of the ITSM framework and the other initiatives follows.

### *Department IT Strategic Management Framework*

#### ITSM Phases

The Department ITSM Framework is designed to establish a Department-wide ITIM process in three phases: IT Planning, IT Funding and Architecture, and IT Investment Oversight.

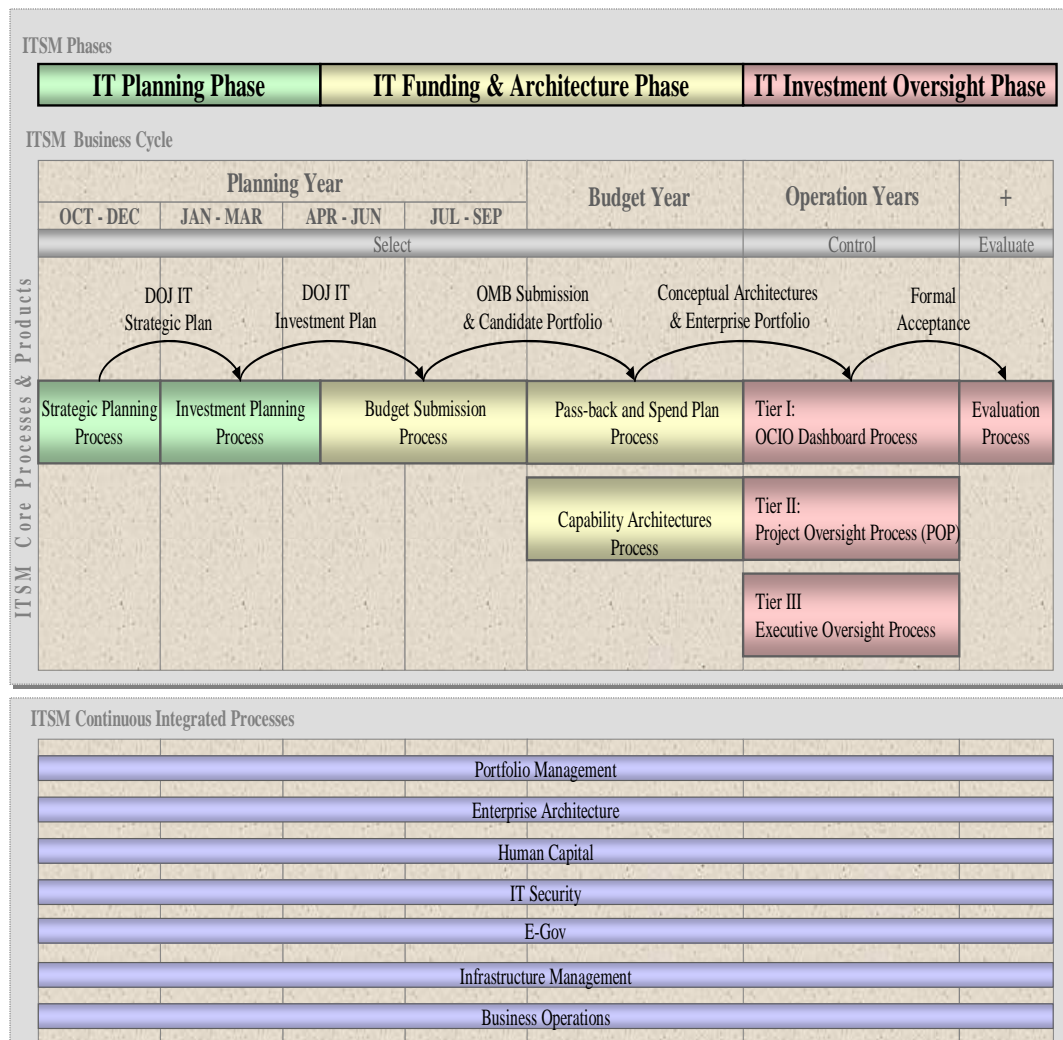
- The IT Planning Phase is to establish the IT strategies and priorities through the development of an IT Strategic Plan and then build on those strategies through the development of an IT Investment Plan.
- The IT Funding and Architecture Phase builds from the IT Planning Phase. The IT Investment Plan is used to formulate a budget, while the architecture portion of the phase develops a "conceptual architecture" to guide project development. The main product of the IT Funding and Architecture Phase is a funded enterprise portfolio.
- The IT Investment Oversight Phase monitors the progress of development and implementation of the Department's IT investments. This phase consists of a continuing evaluation of the Department's IT portfolio to determine whether investments should be made, existing systems should continue to operate, or systems should be eliminated.

---

<sup>11</sup> To attain a higher stage of maturity, an agency must meet certain requirements for that stage in addition to meeting all of the requirements for the previous stages.

As shown in the following ITSM framework model, the three phases are applied to business cycles and are supported by core processes and products, an enterprise portfolio, and performance measures. A discussion of the Department's efforts to implement the model follows.<sup>12</sup>

### IT Strategic Management (ITSM) Framework – Framework Model



DOJ Office of the CIO

Source: Department of Justice, Office of the Chief Information Officer

<sup>12</sup> For a summary of the ITSM Continuous Integrated Processes, see Appendix 9.

### IT Planning Phase

The Strategic Planning Process, part of the IT Planning Phase, identifies the long range goals, objectives, strategies, and measures of



- created an IT Annual Needs Chart to outline major IT issues that will surface over the next couple of years; and
- updated the IT Strategic Plan after 3 years to include performance measurement criteria and align the plan with the Department's mission.

The Department completed its IT Investment Plan in May 2005 and is currently updating the plan for submission to the OMB for the next budget cycle. In FY 2006 and beyond, the Department plans to work on processes and products related to the Strategic, Transition, and Investment plans and develop a Human Capital Plan.

### IT Strategic Planning Process

The Department has recognized the need to focus more attention on IT management and information sharing. As a result, the Department has decided to take a more proactive role in matching technology to identified business needs. Instead of a decentralized approach whereby only the Department components develop ITIM processes, the Department wants to develop a more centralized approach to IT management by developing Department-level ITIM processes. This approach requires components without an ITIM system to use the Department's ITSM framework, while components with established ITIM processes will need to integrate the Department's ITIM processes with their own. The plan's three main goals are to provide: (1) information sharing among all components, (2) a reliable and cost-effective infrastructure to conduct Department-wide electronic business, and (3) management processes and policies to support and improve the Department's IT performance and continuity.

The Department's IT Strategic Plan is based on the 2003 IT Strategic Planning Guide. The strategic goals listed in the IT Strategic Plan include the following.

- Information sharing: to provide quality electronic solutions that allow mission information to be shared in a timely manner inside and outside the Department.
- Infrastructure and Security Services: to provide a seamless, reliable, secure, and cost-effective infrastructure for conducting Department-wide electronic business.
- IT Management: to establish, institute, and improve management processes and policies to support and improve the Department's IT performance and process.

## Investment Planning Process

The Investment Planning Process identifies specific investments needed to achieve the strategic priorities of the Department consistent with the IT Strategic Plan, and seeks to create an investment plan that balances business priorities and funding resources. Using the IT Strategic Plan and the investment plans from portfolio managers and the components, IT planners and business leaders prioritize needed investments. The Department IT Investment Plan is the result of this investment planning. The Investment Plan identifies the recommended IT investments to support the IT Strategic Plan and the investment performance measures that define the expected business results. The Investment Planning Process provides a method for converting the strategic goals and objectives defined by the IT Strategic Plan into a set of prioritized investments for the future.

For the Investment Planning Process, the Department developed a draft investment process guide, an investment plan with performance metrics, portfolio strategies, and a Transition Planning Process Guide. Additionally, IT questionnaires and surveys from component CIOs were collected to determine human capital needs. The development of the Human Capital Plan is ongoing and involves performing the analysis, planning, and organizational transitions needed to staff and manage IT investment portfolios and approved projects. Additionally, the skills and staffing needed to implement the IT initiatives to be funded are assessed, and the actions required to budget for, reassign, acquire, develop, and retain human resources are performed. To date, the Department appears to be making progress toward completing the Investment Planning Process.

## IT Funding and Architecture Phase

The IT Funding and Architecture Phase of the Department's ITSM framework consists of ongoing processes that establish the budget and architectures to be used by the Department and its components in developing, operating, or terminating IT projects. Funding for IT projects follows the same process the Department uses to obtain funding for all other functions: the Budget Submission Process. This process converts the IT Investment Plan into a fully documented and properly formatted IT budget request ready to be combined with the Department's full budget request. This involves the development of investment business cases and other documentation from Department staffs, components, and other sources, and the integration of these individual investments into a unified portfolio for review by the Department's leadership and submission to OMB.

The subsequent pass-back from OMB and Spend Plan Process, as part of the IT Funding and Architecture Phase, leads proposed investments through the budget process to become incorporated into the enterprise portfolio. This occurs through three steps: (1) the OMB pass-back, which provides the Department with initial OMB budget decisions; (2) the submission of the final Department budget, which is then incorporated into the fiscal year budget by the OMB; and (3) the revision of the IT candidate portfolio and preparation of spending plans after the fiscal year budget is enacted. Once funded, the candidate investments are moved to the enterprise portfolio for investment management. The enterprise portfolio contains all of the funded IT investments for the Department.

In the Capability Architectures process, project managers work toward converting the strategies defined in the strategic planning process into an overall Enterprise Architecture. Capability architectures are used by the project managers to drive the development of solution architectures for investment projects. These capability architectures, which focus on providing Enterprise Architecture capabilities for Department-wide support of business needs, are also used to review solution architectures to ensure compliance with initial conceptual architectures.

According to Department officials, the objective for Enterprise Architecture efforts in FY 2003 and prior years was to build a foundation to develop a mature Enterprise Architecture. Business, System, and Data Architectures were developed along with an Enterprise Architecture Management Systems Tool. For the FY 2004 budget, requests for investment and project funding were submitted to the Department by project managers. The Attorney General's IT Budget Guidance, which is a memorandum initiating the annual Department budget process, was also developed for funding the Department's IT projects. For FY 2005, an integrated budget submission process was developed and, according to Department officials, this process allowed the Department to work closely with the JMD Budget Staff to integrate Department IT needs into the budget. For FY 2006 and future years, the Department intends to institutionalize an integrated budget submission process. However, the actual processes and policies have not yet been determined. Additionally, a Budget Submission Guide and a performance measurement document are still needed to complete the IT Funding and Architecture Phase.

#### IT Oversight Phase

As mandated by Clinger-Cohen, each agency head must establish ITIM processes and provide oversight by determining: (1) which employees should perform certain IT management functions; (2) if certain IT functions

should be contracted to outside sources; (3) which IT missions, processes, and administrative practices must be revised to support each other in making significant investments; and (4) if the information security policies, procedures, and practices are adequate.

In complying with the oversight responsibilities outlined in Clinger-Cohen, Department Order 2880.1A stated that the Department's CIO is responsible for:

- developing and implementing Department ITIM policy and guidance;
- confirming that each Department component has a decision-making infrastructure and appropriate ITIM processes in place to make sound business investments based on thorough planning, risk management, project prioritization, and funding availability;
- assisting components in developing and implementing ITIM processes and providing value-added services or information on cross-cutting issues or investments;
- ensuring Department IT investments are consistent with Department IT strategic planning, budget, acquisition, and program management decisions;
- supporting the IT Investment Board and CIO Council in performing their duties;
- performing oversight of components' IT investments and ITIM processes through the annual budget process, independent technical assessments, and regularly scheduled briefings on the components' portfolios and the individual IT investments within the portfolios;
-

In response to Order 2880.1A, issued in March 2001, 29 of the 34 major components required to submit ITIM processes to the Department complied by September 2002.<sup>14</sup> Five components did not submit an ITIM process for approval, while another five components that were not required to submit a process submitted one. None of the ITIM processes were fully developed. According to a Department IT official, the five components that did not submit ITIM processes were small and did not have significant IT investments. Initially, the Department tracked whether the components submitted ITIM processes and whether the processes were approved by the Department's CIO. The Department responded to the components, stating that their ITIM processes would be evaluated and either accepted or rejected. The Department then provided suggestions for improving their processes. In addition, the Department surveyed the components in May 2003, nearly 1 year after the ITIM processes were submitted, to determine how the components had progressed. According to the Department CIO, the components were having a difficult time developing their ITIM processes and progress was slow. In JMD's case, its efforts begun in 2002 to develop component-level ITIM processes were abandoned in 2004 as it focused on developing the ITSM framework for the Department's overall ITIM effort. The Department is planning to issue a revised version of Order 2880.1A which is expected to better outline component responsibility as well as the Department's oversight role. The Department does not have an estimated date for issuance of the revised version.

For the components considered by the Department to be so small that it would not be beneficial to spend time developing a component-based ITIM process, yet they have IT systems necessitating an ITIM process, the Department developed what it refers to as an "ITIM-lite" process to facilitate decision making throughout the life cycle of an IT project. The purpose of ITIM-lite was to allow management to:

- select the most worthwhile projects through systematic review of new and ongoing investments,
- control the investments to ensure they are appropriately managed to deliver the benefits promised, and
- evaluate the investments to validate that they deliver what is expected.

---

<sup>14</sup> 28 C.F.R. lists 35 components, but we did not include the Office of International Programs because it is no longer part of the Department of Justice.

The Department abandoned ITIM-lite and in 2004 began developing its Department-wide ITIM processes, which are expected to encompass the smaller components.

The Department has not recently been overseeing the development of components' ITIM processes. Instead, the Department decided to concentrate its oversight attention on components' actual investments. The one exception, according to Department officials, is the tracking of the FBI's development of ITIM processes because the FBI accounts for about 50 percent of the Department's IT budget. Oversight of the development of other components' ITIM processes was abandoned in 2002. The Oversight Phase in the ITSM Framework, as discussed below, involves monitoring components' IT projects rather than overseeing or approving components' ITIM processes or the development of the processes. According to the Department CIO, oversight of the components' ITIM processes is currently performed on an ad hoc basis.

According to the ITSM framework, project oversight will occur during the operational years of IT projects and will be divided into three tiers: the Department Dashboard Process (Tier 1), the Project Oversight Process (Tier 2), and the Executive Oversight Process (Tier 3).

The Department Dashboard (Tier 1) is a query tool that provides users with the ability to access a database of Department components' IT systems using a web browser interface. The Dashboard is designed to provide the Department, component CIOs, and project managers with a "quick reference" on the current cost, schedule, performance, and risks for major or highly visible component investment projects that are in the Department's IT portfolio. Projects are identified as being in a state of completion, planning, operation, or on hold to be reviewed by the Department CIO. The Department Dashboard gives component project managers and reviewers access to IT project data. Data in the Dashboard includes project cost, schedule performance, and risks. The Dashboard is accessible through the Department Intranet.

Project managers record the risks, milestones, and costs of projects into the Dashboard. Based on the risks associated with the project, the project manager rates the status of the project as red, yellow, or green. Issues regarding excessive cost or funding shortfalls are rated red. Issues with the potential to have excessive costs or funding shortfalls are rated with a yellow status. If there are no excessive cost issues, projects are rated green. Department officials then review the project information in the Dashboard, paying special attention to projects designated as red or yellow. Project managers are required to update the status of their projects by the

10<sup>th</sup> business day of each month. However, the project managers can bring a project to the attention of the Department CIO at any time. The Dashboard flags any changes made in baseline data and then displays the project with a red flag. A Department Dashboard official can then follow up with inquiries to the project managers. The Dashboard categorizes projects by component. Once the Dashboard is reviewed by the component CIO and the Dashboard Policy Advisor, the Department CIO reviews it. The CIO then holds meetings to discuss the status of projects. Currently all components, with the exception of the FBI, are connected to the Dashboard, which covers approximately 80 investments. Project managers are involved in the process through training sessions, a user guide, and one-on-one meetings as necessary.

The Project Oversight Process (Tier 2) will consist of approximately 12 to 15 projects that are selected from those in the first tier for review and face-to-face meetings with project managers to make sure the projects are meeting their expected performance. The projects selected for this tier are those that may be high-risk, over budget, politically sensitive, or otherwise demand closer scrutiny. A Department official explained that this is the level at which members of the IT and Policy and Planning Staff in the Department will become directly involved.

In the third tier, the Executive Oversight Process, approximately six projects will be selected from Tier 2, based on Department or congressional priorities, for evaluation from an investment, business, and return-on-investment perspective. This process is carried out by the Department Executive Review Board (DERB) assembled at the level of the CIO, Controller, and Deputy Attorney General. This process began as a pilot program, but its scope is now being expanded to include the Department's entire portfolio.

According to the GAO's ITIM framework, instituting IT investment boards is a key component in the IT investment management process because the boards define the membership, guiding policies, operations, roles, responsibilities, and authorities for each designated board and, if appropriate, each board's support staff. Prior to the establishment of the DERB in 2004, various committees and boards were formed to facilitate the sharing of information between the Department and its components, including the following.

- The CIO Council, comprised of representatives of the major components, monitored cross-cutting investments and provided

technical expertise to the Department CIO and Senior Management Council.<sup>15</sup>

- The Enterprise Architecture Committee, comprised of the Chief Architects of the major components, held monthly meetings with the CIO Council to discuss investment progress.
- The Data Architecture Sub-Committee ensured that data standards conformed with the Enterprise Data Architecture. Specifically, the committee supported transitioning from stovepiped information systems to a shared data environment.

By the end of FY 2003, all but the CIO Council were disbanded and replaced with the DERB, which is now responsible for reviewing the major IT investments of all components.

A DERB official explained that investments are selected for review based on an investment's budget or the mission-critical nature of the investment. In terms of budget, two types of projects will be reviewed: projects that are to run for more than 10 years and funded at more than \$20 million, or short-term projects running for about 1 year with a budget of at least \$15 million. Projects considered to be mission-critical or strategically important for the Department are reviewed, even though they may not be costly, because of the high risk involved with meeting the Department's mission. The DERB's Department-level oversight occurs in meetings where members discuss the investments as well as the planning, budget, risk, and assessment of current component projects. The first official DERB meeting was in November 2004 and since its inception, the DERB has met approximately five times. We found that while the DERB contributes to the cohesive nature of the ITSM framework, it is neither as comprehensive in its functions nor as capable of devoting sufficient time to individual projects as the disbanded boards that were designed to be tailored to specific IT resources.

## **Conclusion**

The Clinger-Cohen Act and OMB Circular A-130 require agencies to ensure that IT investments are made with an overall focus on the agency's mission and with senior management oversight. When ITIM processes using a select, control, and evaluate methodology are performed properly, the

---

<sup>15</sup> The CIO Council includes the designated CIOs who were represented on the Department's Strategic Management Council, including the Federal Bureau of Prisons, FBI, DEA, and Civil Division.



agency should reduce the risk and maximize the benefits from IT investments.

In March 2001, the Department issued Order 2880.1A, which required its components to implement ITIM methodologies and submit these methodologies for review by the Department CIO. The Department also provided guidance for developing ITIM processes. The Department planned to rely on the components' submissions to meet ITIM requirements. While most components submitted ITIM plans, progress was slow to implement ITIM processes. This strategy did not provide the components with a clear vision of how they should create their ITIM processes to meet the overall mission of the Department, as the Department did not have a fully developed IT Strategic Plan or Enterprise Architecture that would outline the overall mission of the Department and identify the IT investments that should be made to achieve that mission.

In 2004 the Department developed the ITSM framework, which was designed to lead to Department-level ITIM processes. In our judgment, the ITSM framework can result in fully mature ITIM processes if carried out properly. The Department's ITSM Framework includes the funding, oversight, and planning requirements outlined in the Clinger-Cohen Act. The Department has made some progress in implementing the processes outlined in its ITSM. Still, not all of the processes have been implemented. For example, the Investment Planning Guide and enterprise portfolio are two key elements of the ITSM that are not yet fully implemented. Without these elements, the Department cannot provide components with a complete picture of what investments should be pursued. Additionally, it is not clear that all of the Department's IT investments will be adequately covered by the ITSM.

We believe that if the Department's ITSM is successfully implemented, mature ITIM processes will result. However, at this early stage it is difficult to assess whether all the components will have developed compatible ITIM processes or be covered adequately by the Department's ITIM processes. Major components, such as the DEA and FBI, are well ahead of the Department and its ITSM development.

The ultimate success of the Department's current efforts to develop mature ITIM processes is difficult to evaluate at this early stage. The effort is likely to take years, and the Department has no firm schedule for developing its ITIM processes or ensuring the development of compatible component-level ITIM processes. In the meantime, the Department risks investing in or maintaining systems that are duplicative or may need to be

replaced, altered, or eliminated if they do not align with the mission and the goals of the Department.

## **Recommendations**

We recommend that JMD:

4. Fully implement the phases outlined by the ITSM framework to ensure that all Department IT investments are covered by an ITIM process.
5. Ensure that components requiring ITIM processes develop them.
6. Provide assistance to components in developing and implementing ITIM processes and providing value-added services.
7. Establish a clear schedule for the completion of the ITSM framework and the completion of a mature ITIM process.

## **STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS**

We have audited the Department's management of Enterprise Architecture and IT investments. The audit was conducted in accordance with Government Auditing Standards. As required by the standards, we reviewed management processes and records to obtain reasonable assurance about the Department's compliance with laws and regulations that, if not complied with, in our judgment could have a material effect on Department operations. Compliance with laws and regulations applicable to the Department's handling of Enterprise Architecture and IT investments is the responsibility of the Department's management.

Our audit included examining, on a test basis, evidence about laws and regulations. The specific laws and regulations against which we conducted our tests are contained in the relevant portions of the Clinger-Cohen Act of 1996, OMB Circular A-11 § 300, and OMB Circular A-130.

The Clinger-Cohen Act of 1996:

- as applied to Enterprise Architecture, requires the CIOs for major departments and agencies to develop, maintain, and facilitate the implementation of architectures as a means of integrating business processes and agency goals with IT; and
- as applied to ITIM, defines requirements for capital planning and control of IT investments and mandates a select/control/evaluate approach that federal agencies must follow.

OMB Circular A-11, § 300:

- as applied to ITIM, establishes the criteria for completing Exhibits 300, which is the format used to represent the purpose for the proposed investment to agency management and the OMB.

OMB Circular A-130:

- as applied to Enterprise Architecture, requires agencies to create an Enterprise Architecture Framework; once a framework is established, an agency must create and maintain an Enterprise Architecture; and

- as applied to ITIM, defines requirements for capital planning and control of IT investments using a select/control/evaluate approach.

As noted in the Finding and Recommendations section of our report, the Department has not yet established an Enterprise Architecture or ITIM processes and therefore is not in compliance with the Clinger-Cohen Act, OMB guidance, and Department regulations. However, the Department is actively developing and implementing new frameworks aimed at establishing an Enterprise Architecture and ITIM processes in the future. Also, some Department components, such as the FBI and the DEA, have made progress in developing component-level Enterprise Architectures and ITIM processes.

## **STATEMENT ON INTERNAL CONTROLS**

In planning and performing our audit of the Department's management of its Enterprise Architecture and IT investments, we considered the Department's internal controls for the purpose of determining our audit procedures. This evaluation was not made for the purpose of providing assurance on the internal control structure as a whole. However, we noted certain matters that we consider to be reportable conditions under Government Auditing Standards.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the internal control structure that, in our judgment, could adversely affect the Department's ability to manage its Enterprise Architecture and IT investments. During our audit, we identified the following internal control concerns.

- The Department has not yet completed an Enterprise Architecture to drive its IT investments.
- The Department has not yet implemented the control and evaluate processes necessary to complete its IT investment capability.
- The Department does not provide adequate oversight of components' Enterprise Architecture and ITIM efforts.

Because we are not expressing an opinion on the Department's internal control structure as a whole, this statement is intended solely for the information and use of the Department in managing its Enterprise Architecture and IT investments. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

**OBJECTIVE, SCOPE, AND METHODOLOGY**

**Objective**

The objective of the audit was to determine whether the Department is effectively managing its Enterprise Architecture and IT investments.

**Scope and Methodology**

The audit was performed in accordance with Government Auditing Standards, and included tests and procedures necessary to accomplish the audit objectives. We conducted work at the Department and its Justice Management Division in Washington, D.C.

To perform our audit, we interviewed Department and GAO officials, and reviewed documents related to Enterprise Architecture and IT management policies and procedures, project management guidance, strategic plans, IT project proposals, budget documentation, organizational structures, and prior GAO and OIG reports.

To determine the Department's progress in developing an Enterprise Architecture, we used the GAO's Enterprise Architecture Management framework as criteria. As part of our assessment of the Department's Enterprise Architecture, the Department completed a survey developed by the GAO to identify which of the core elements in the GAO's Enterprise Architecture Management framework were implemented. We reviewed the survey and obtained supporting documentation for the core elements that the Department said were implemented. We did not test or review documentation for the core elements that the Department considered not implemented or partially implemented.

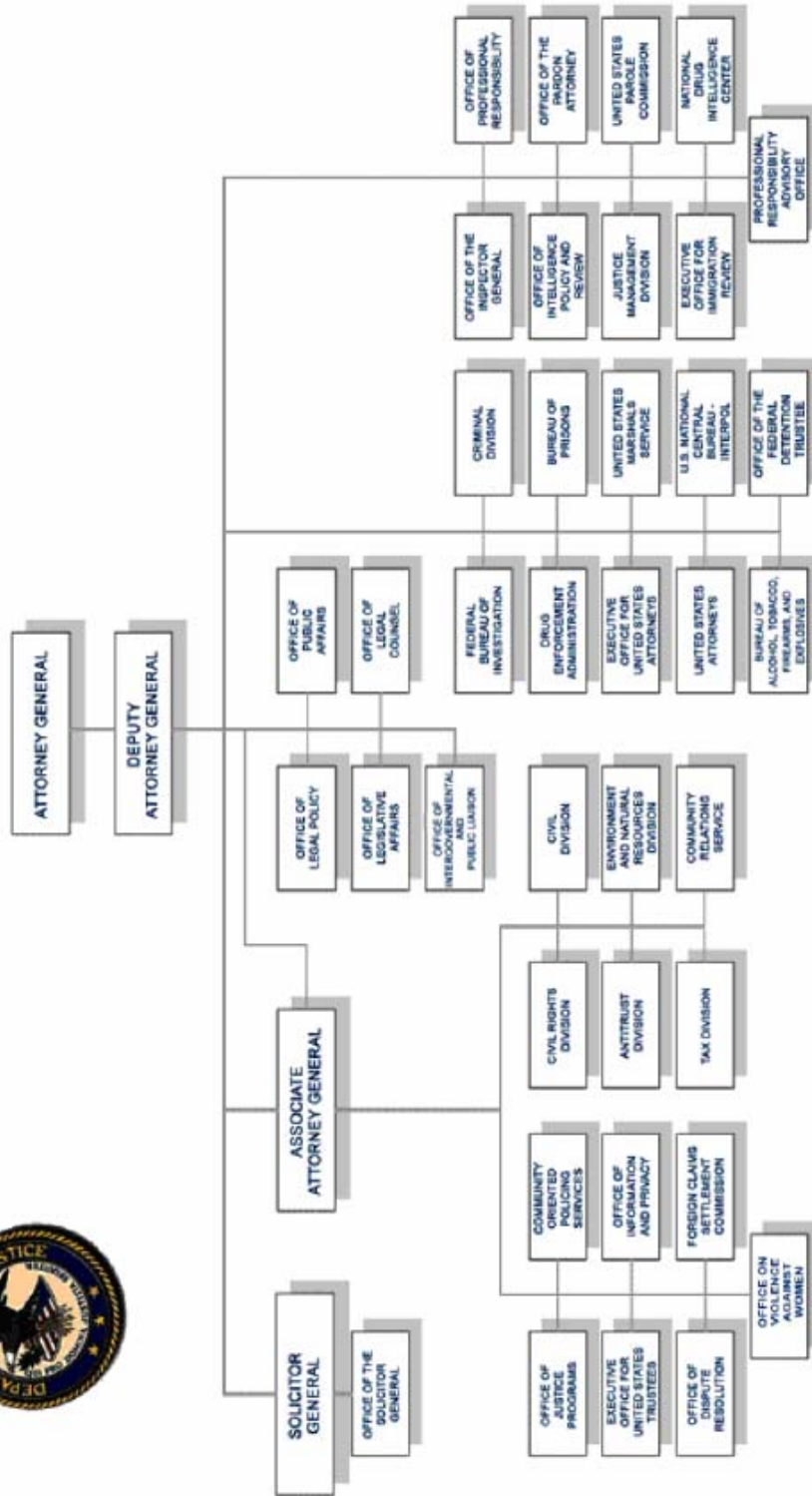
To determine whether the Department is effectively managing its IT investments, we reviewed the GAO's ITIM framework in relation to the Department's ITSM and also the Department's regulations, IT policies and procedures, program managers' presentations, meeting minutes, training agenda, and other information. Based on interviews and our review of documentation provided by Department officials, we determined the status of their efforts to develop ITIM processes.

To determine whether the Department was providing effective oversight to its components' Enterprise Architecture and ITIM efforts, we

reviewed DOJ Order 2880.1A and determined through interviews and documentation the extent to which those efforts were formally guided and monitored.



# DEPARTMENT OF JUSTICE

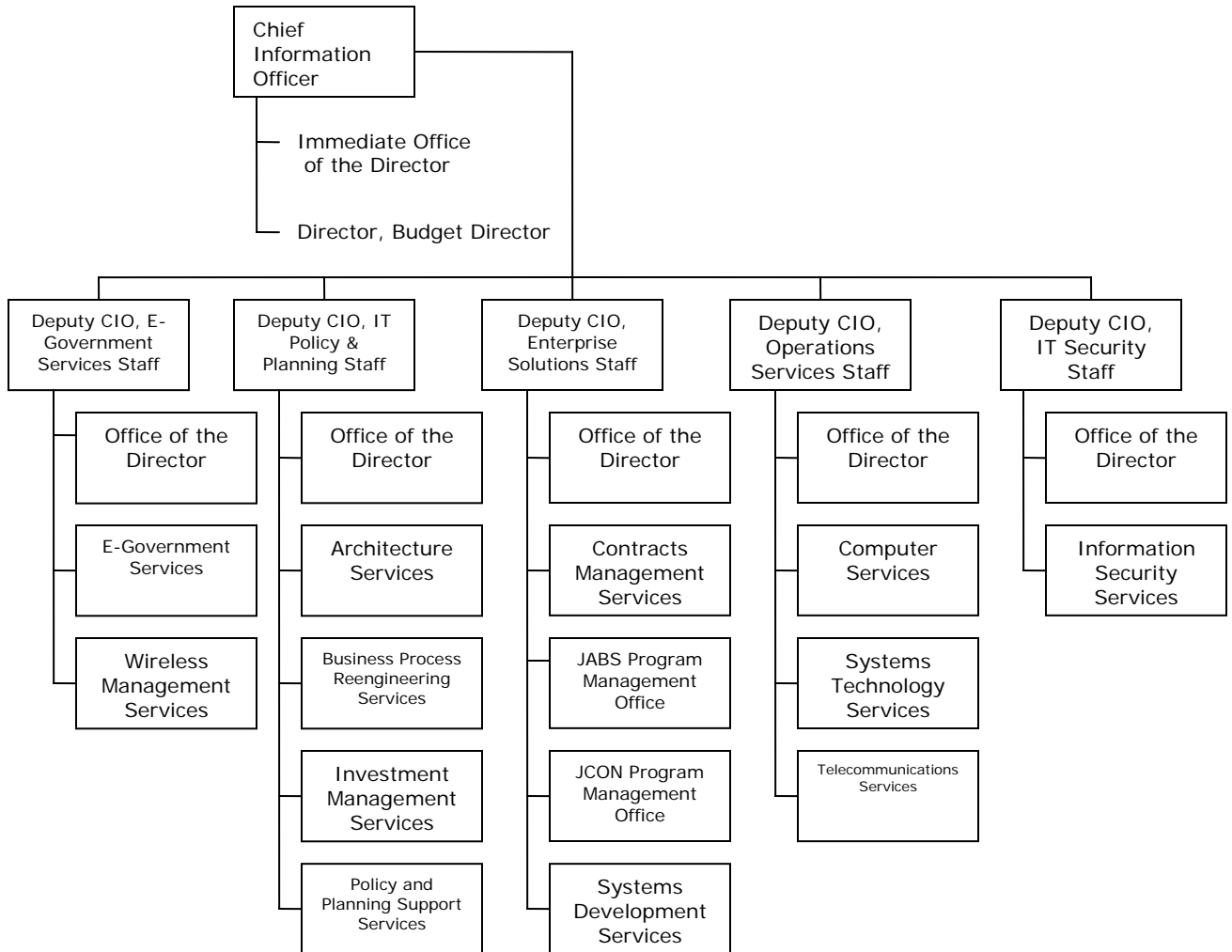


## APPENDIX 2

Approved by: *John D. Ashcroft* Date: 7-14-03  
JOHN D. ASHCROFT  
Attorney General



# DEPARTMENT OF JUSTICE OFFICE OF THE CHIEF INFORMATION OFFICER



Source: Justice Management Division

**ACRONYMS**

ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CTO	Chief Technology Officer
DEA	Drug Enforcement Administration
DERB	Department Executive Review Board
DOJ	Department of Justice
EA	Enterprise Architecture
EAC	Enterprise Architecture Committee
FBI	Federal Bureau of Investigation
FEAF	Federal Enterprise Architecture Framework
FEAMS	Federal Enterprise Architecture Management System
FY	Fiscal Year
GAO	Government Accountability Office
IRM	Information Management Resources
IT	Information Technology
ITIM	Information Technology Investment Management
ITSM	Information Technology Strategic Management
JCON	Justice Consolidated Office Network
JMD	Justice Management Division
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
O&M	Operations and Maintenance
OMB	Office of Management and Budget
PKI	Public Key Infrastructure
SDLC	Systems Development Life Cycle
TRM	Technical Reference Model
UFMS	Unified Financial Management System

## APPENDIX 4

### SUMMARY OF ENTERPRISE ARCHITECTURE MANAGEMENT FRAMEWORK'S MATURITY STAGES, CRITICAL SUCCESS ATTRIBUTES, AND CORE ELEMENTS

	Stage 5:				
	Stage 3: Developing EA products			Stage 4: Completing EA products	Leveraging the EA to manage change
	Stage 1: Creating EA awareness	Stage 2: Building the EA management foundation			
Attribute 1: Demonstrates commitment		Adequate resources exist. Committee or group representing the enterprise is responsible for directing, overseeing, or approving EA.	Written and approved organization policy exists for EA development.	Written and approved organization policy exists for EA maintenance.	Written and approved organization policy exists for IT investment compliance with EA.
Attribute 2: Provides capability to meet commitment		Program office responsible for EA development and maintenance exists. EA is being developed using a framework, methodology, and automated tool.	EA products are under configuration management.	EA products and management processes undergo independent verification and validation.	Process exists to formally manage EA change. EA is integral component of IT investment management process.
Attribute 3: Demonstrates satisfaction of commitment		EA plans call for describing both the “as is” and the “to-be” environments of the enterprise, as well as a sequencing plan for transitioning from the “as is” to the “to-be.” EA plans call for describing both the “as is” and the “to-be” environments in terms of business, performance, information/data, application/service, and technology descriptions to address security.	EA products describe or will describe both the “as is” and the “to-be” environments of enterprise, as well as a sequencing plan for transitioning from the “as is” to the “to-be.” Both the “as is” and the “to-be” environments are described or will be described in terms of business, performance, information/data, application/service, and technology. Business, performance, information/data, application/service, and technology descriptions address security.	EA products describe both the “as is” and the “to-be” environments of enterprise, as well as a sequencing plan for transitioning from the “as is” to the “to-be.” Both the “as is” and the “to-be” environments are described in terms of business, performance, information/data, application/service, and technology. Business, performance, information/data, application/service, and technology descriptions address security. Organization CIO has approved current version of EA. Committee or group representing the enterprise or the investment review board has approved current version of EA.	EA products are periodically updated. IT investments comply with EA. Organization head has approved current version of EA.
Attribute 4: Verifies satisfaction of commitment		EA plans call for developing metrics for measuring EA progress, quality, compliance, and return on investment.	Progress against EA plans is measured and reported.	Quality of EA products is measured and reported.	Return on EA investment is measured and reported. Compliance with EA is measured and reported.

Maturation →

Note: Enterprise Architecture (EA)

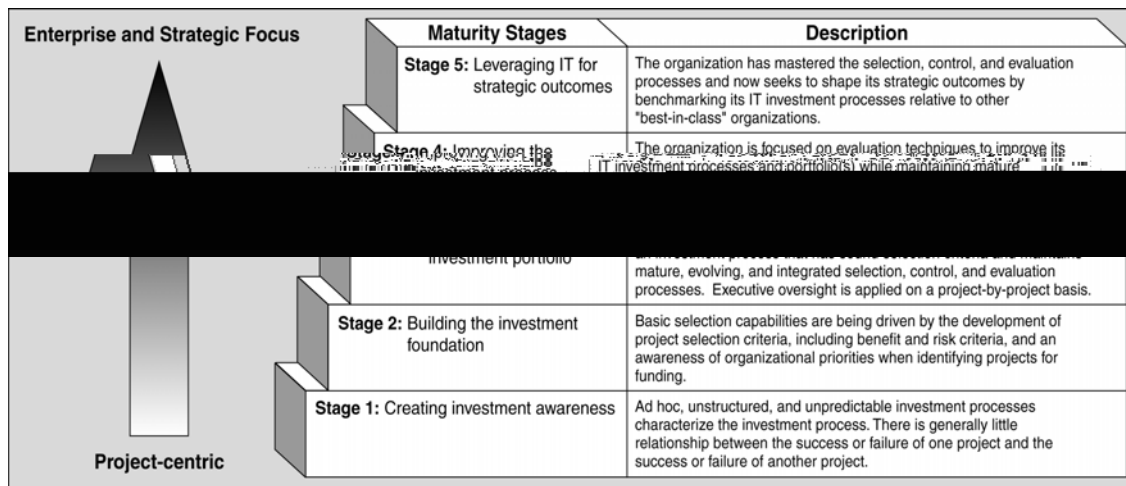
Source: Government Accountability Office

## APPENDIX 5

## SUMMARY OF GAO ITIM FRAMEWORK

The ITIM framework is a hierarchical model comprised of five maturity stages. Each stage builds upon the lower stages and represents a step toward achieving both stable and effective ITIM processes. A summary of the five stages is presented below.

### THE FIVE ITIM MATURITY STAGES



Source: Government Accountability Office

Stage 1 describes the state of an organization prior to any framework implementation and does not contain critical processes. Maturity stages 2 through 5 are composed of a series of critical processes, each of which must be implemented and institutionalized for an organization to satisfy stage requirements and advance to the next stage. The ITIM framework also breaks down each critical process into a set of key practices. Key practices are specific tasks and conditions that must be in place for an organization to implement effectively the necessary critical processes. A summary of ITIM critical processes for each maturity stage is presented in the following chart.

## CRITICAL PROCESS SUMMARIES

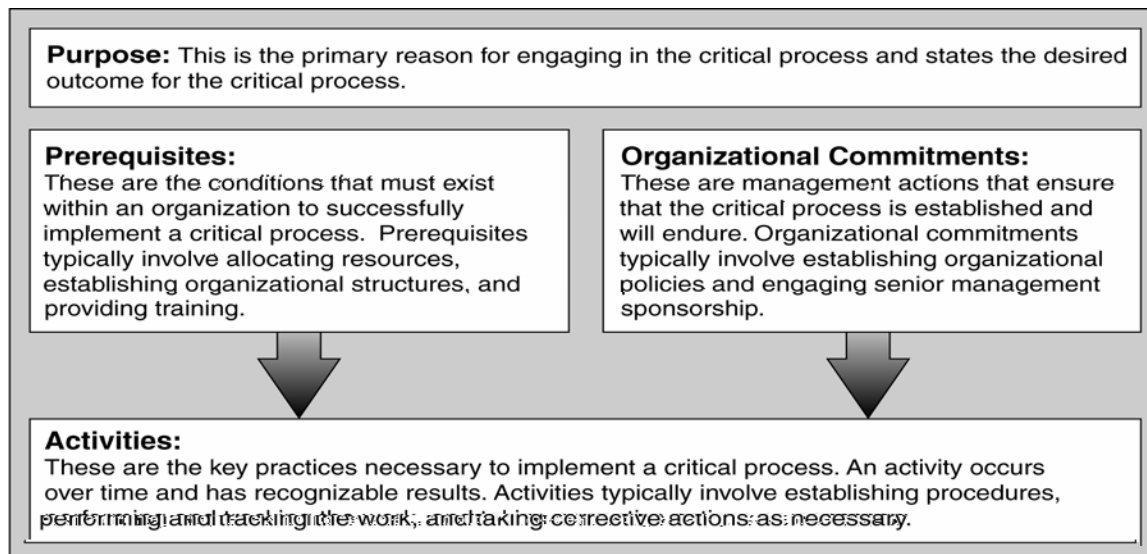
Maturity stages	Critical processes
<b>Stage 5:</b> Leveraging IT for strategic outcomes	<ul style="list-style-type: none"> <li>- Optimizing the investment process</li> <li>- Using IT to drive strategic business change</li> </ul>
<b>Stage 4:</b> Improving the investment process	<ul style="list-style-type: none"> <li>- Improving the portfolio's performance</li> <li>- Managing the succession of information systems</li> </ul>
<b>Stage 3:</b> Developing a complete investment portfolio	<ul style="list-style-type: none"> <li>- Defining the portfolio criteria</li> <li>- Creating the portfolio</li> <li>- Evaluating the portfolio</li> <li>- Conducting postimplementation reviews</li> </ul>
<b>Stage 2:</b> Building the investment foundation	<ul style="list-style-type: none"> <li>- Instituting the investment board</li> <li>- Meeting business needs</li> <li>- Selecting an investment</li> <li>- Providing investment oversight</li> <li>- Capturing investment information</li> </ul>
<b>Stage 1:</b> Creating investment awareness	<ul style="list-style-type: none"> <li>- IT spending without disciplined investment processes</li> </ul>

Source: Government Accountability Office

Four core elements comprise each critical process in the ITIM framework. These elements indicate whether the implementation and institutionalization of a process can be effective and repeated. The four core elements outlined in the ITIM framework are: (1) purpose,

- (1) organizational commitment, (3) prerequisites, and (4) activities. The following chart illustrates the relationship between the four core elements.

## THE FOUR CRITICAL PROCESS ELEMENTS



Source: Government Accountability Office

Each core element, except for the “purpose” core element, contains specific key practices. The ITIM framework states that these key practices are the attributes and activities that contribute most to implementing and standardizing a critical process.

## APPENDIX 6

### DEPARTMENT PROGRESS THROUGH STAGE 3 OF THE ENTERPRISE ARCHITECTURE MANAGEMENT FRAMEWORK

Core Elements	Status	
	<i>Implemented</i>	<i>Not Implemented</i>
<b>STAGE 2</b>		
<b>Critical Attribute #1: Demonstrates Commitment</b>		
Adequate Resources		✓
Enterprise Architecture Governing Committees		✓
<b>Critical Attribute #2: Capability to Meet Commitment</b>		
Enterprise Architecture Program Office	✓	
Appointment of Chief Architect	✓	
Enterprise Architecture Development Using a Framework, Methodology, and Automated Tool		✓
<b>Critical Attribute #3: Demonstrates Satisfaction of Commitment</b>		
Enterprise Architecture Program Plan Development	✓	
Security	✓	
<b>Critical Attribute #4: Verifies Satisfaction of Commitment</b>		
Enterprise Architecture Progress Measurement		✓
<b>STAGE 3</b>		
<b>Critical Attribute #1: Demonstrates Commitment</b>		
Enterprise Architecture Development Policy		✓
<b>Critical Attribute #2: Capability to Meet Commitment</b>		
Enterprise Architecture Products Under Configuration Management		✓
<b>Critical Attribute #3: Demonstrates Satisfaction of Commitment</b>		
Develop "As-is," "To-be," and Transition Architectures		✓
Security	✓	

Core Elements	Status	
	<i>Implemented</i>	<i>Not Implemented</i>
<b>Critical Attribute #4: Verifies Satisfaction of Commitment</b>		
Measure and Report Enterprise Architecture Progress		✓

Source: Office of the Inspector General.



### THE THREE COMPONENTS OF THE ITIM PROCESS

#### Select Phase

In the Select phase of the capital planning and investment control process, A-130 requires agencies to:

- determine whether the investment will support core mission functions;
- demonstrate a projected return on investment that is clearly equal to or better than alternative uses of available public resources;
- prepare and update a benefit-cost analysis for each information system through its life cycle;
- prepare and maintain a portfolio of major information systems;
- ensure consistency with federal, agency, and bureau Enterprise Architectures;
- ensure investments are not duplicative; and
- establish oversight mechanisms to ensure the continuing security, interoperability, and availability of systems and data.

#### Control Phase

In the Control phase of the capital planning and investment control process, A-130 requires agencies to:

- institute performance measures and management processes that monitor actual performance compared to expected results;
- establish oversight mechanisms to determine whether information systems continue to fulfill ongoing and anticipated mission requirements;
- ensure that information systems meet established milestones, deliver intended benefits, meet user requirements, and identify and offer security protections;

- prepare and update a strategy that identifies and mitigates risks associated with each information system; and
- ensure that agency Enterprise Architecture procedures are followed.

### Evaluate Phase

In the Evaluate phase of the capital planning and investment control process, A-130 requires agencies to:

- conduct post-implementation reviews of information systems and information resource management processes to validate estimated benefits and costs and document effective management practices for broader use;
- evaluate systems to ensure positive return on investment and decide whether continuation, modification, or termination of the systems is necessary to meet agency mission requirements;
- document lessons learned from the post-implementation reviews, and redesign oversight mechanisms and performance levels to incorporate acquired knowledge;
- re-assess an investment's business case, technical compliance, and compliance against the Enterprise Architecture; and
- update the Enterprise Architecture and IT capital planning processes as needed.

## PRIOR REPORTS

We identified eight IT-related reports issued since May 2000 by the GAO and the OIG that are relevant to this audit. In May 2000, the GAO reported that although almost all federal agencies had created some type of ITIM process, none had yet implemented stable processes addressing all three phases of the select-control-evaluate approach.<sup>16</sup> According to the GAO, one barrier to implementing reliable ITIM has been the lack of specific guidance on the required processes.

In February 2002, the GAO reported that the federal government as a whole had not reached a mature state of Enterprise Architecture management.<sup>17</sup> In particular, about 52 percent of federal agencies reported having at least the management foundation that is needed to begin successfully developing, implementing, and maintaining an Enterprise Architecture, but about 48 percent of agencies had not yet advanced to this basic stage of maturity. In November 2003, the GAO updated its 2002 report and concluded that little progress had occurred in agencies' Enterprise Architecture management.<sup>18</sup>

In April 2002, pursuant to the FY 2001 Government Information Security Reform Act, the OIG issued a report on JMD's Rockville and Dallas Data Centers IT system. The report identified vulnerabilities with management, operational, and technical controls. The report noted significant vulnerabilities in the following areas:

- security policies and procedures,
- authorization of software changes,
- contingency planning,

---

<sup>16</sup> The report is entitled *Information Technology Investment Management: An Overview of GAO's Assessment Framework* (GAO/AIMD-00-155), dated May 2000.

<sup>17</sup> The report is entitled *Information Technology, Enterprise Architecture Use Across the Federal Government Can Be Improved* (GAO-02-6), dated February 2002.

<sup>18</sup> The report is entitled *Information Technology, Leadership Remains Key to Agencies Making Progress on Enterprise Architecture Efforts* (GAO-04-40), dated November 2003.

- password management,
- logon management,
- account integrity management, and
- system auditing management.

The report stated that these vulnerabilities occurred because JMD lacked sufficient guidance, adequate security policies, and effective enforcement of policies.

In December 2002, the OIG issued a report on the FBI's Management of IT Investments. The OIG reported that the FBI did not have a fully developed enterprise architecture. Also, the FBI was not effectively selecting, controlling, and evaluating its IT investments because it had not fully implemented any of the critical processes necessary for successful ITIM.

In May 2003, also pursuant to the FY 2001 Government Information Security Reform Act, the OIG issued a report on JMD's Justice Communications Network IT system. The report identified vulnerabilities with the IT system including management, operational, and technical controls. The report noted significant vulnerabilities in the following areas:

- review of security controls,
- personnel security,
- contingency planning,
- hardware and system software maintenance,
- documentation,
- identification and authentication, and
- logical access controls.

The report stated that these vulnerabilities occurred because JMD had not implemented Department policies or updated security information and procedures.

In June 2004, pursuant to the Federal Information Security Management Act, the OIG issued an oversight and information systems consolidated report. The report identified JMD vulnerabilities in the following areas:

- vulnerability tracking capability and documented structured compliance evaluation procedures,
- oversight,
- creating specific goals,
- components documenting systems configuration management process for their systems,
- components adequately developing and distributing Rules of Behavior to all employees and contractors prior to the gaining access to the systems, and
- components reporting computer security incidents to the Department of Justice Computer Emergency Response Team in a timely manner.

In September 2004, the OIG issued a report on the Drug Enforcement Administration's Management of Enterprise Architecture and IT Investments. The OIG found that the Drug Enforcement Administration had completed nearly 90 percent of the Enterprise Architecture Management Framework criteria for meeting the second of five levels of maturity. Also, the Drug Enforcement Administration had attained Stage 2 of the five maturity stages outlined in the GAO ITIM Framework.

**DEPARTMENT ITSM FRAMEWORK'S  
CONTINUOUS INTEGRATED PROCESSES**

According to the Department's ITSM framework, IT Investments can be categorized as development projects, Operations and Maintenance (O&M) projects, and management processes. Development projects are those which are either new or undergoing major enhancements. O&M projects are considered steady state, meaning they are fully operational and continue to operate without significant enhancements. Management processes are on-going business operations as opposed to projects with a scheduled start and end date. All three types of investments grow through defined models. Development projects evolve through the Department System Development Life Cycle (SDLC), O&M projects evolve through the Department Operations Analysis Model, and management processes mature according to the Department Process Maturity Model.

The SDLC Model is used to manage system projects. The SDLC, established in 2003, has not yet been updated. According to the ITSM framework, the SDLC will be updated and streamlined to provide the sequence of activities that are needed to support Department-wide project management, oversight, and performance management of development projects. The SDLC will be used to compute the earned value of investment projects as they progress through the system development phases.

### ITSM Core Processes and Products

The ITSM framework phases are composed of core interlocking processes that perform the business of each phase by passing core products from one core process to another. Each core product and process supports the Department enterprise portfolio.

### ITSM Continuous Integrated Processes

The core products of the ITSM framework are the culmination of contributions from other Department business areas: (1) portfolio management, (2) Enterprise Architecture, (3) human capital, (4) information security, (5) E-Gov, (6) infrastructure management, and (7) business operations. Each of these business areas is integrated at the appropriate places in the ITSM core processes to provide substantial input towards the ITSM core products. The ITSM continuous integrated processes and the ITSM framework represent the total workings of the Department.

### ITSM Enterprise Portfolio

The enterprise portfolio, as discussed in Finding 1, is one of the main products of the Department and inventories the Department's IT assets.

The portfolio will be made up of investc -0.0016 Tw 18.1 0 T[ 0 Tartmsliolso.72ferruss

APPENDIX 10

THE DOJ'S RESPONSE TO THE DRAFT REPORT

---



U.S. Department of Justice

Washington, D.C. 20530

OCT 20 2005

MEMORANDUM FOR GLENN A. FINE  
INSPECTOR GENERAL

FROM: Walter E. Hitzel  
Chief Information Officer

SUBJECT: Office of Inspector General Draft Audit Report  
"The Status of Enterprise Architecture and  
Information Technology Investment Management  
in the Department of Justice"

This is in response to the Office of the Inspector General's (IG) request for comments on the draft Fiscal Year 2005 audit report of "The Status of Enterprise Architecture and Information Technology Investment Management in the Department of Justice."

My office has completed it's review of the draft report and has initiated corrective action to address the findings and recommendations identified. The Department is continuing to develop, refine, and implement its Information Technology Investment Management program and is continuing to develop its Enterprise Architecture program. In August 2005, the DOJ Department



2. Increased levels of guidance and coordination with DOJ Component organizations; and
3. Greater maturity with EA efforts, as assessed within the GAO's EAMMF and OMB Effectiveness Assessment.

Below are the responses to the specific recommendations contained in the Report. If you have any questions or require additional information, please feel free to contact Kent Holtgrewe on (202)514.9682 or by email at [kent.holtgrewe@usdoj.gov](mailto:kent.holtgrewe@usdoj.gov), or Kevin Deeley on (202)353-2421 or by email at [kevin.deeley@usdoj.gov](mailto:kevin.deeley@usdoj.gov).)

**Recommendation 1.**


~~Complete the Department wide Enterprise Architecture to insure that IT investments are not duplicative, are well integrated, are cost-effective, and support the Department's mission.~~

**Concur.** The EAPMO Program Management Plan scope will explicitly state that the Enterprise Architecture will be Department wide, fully leveraging as opposed to replacing, existing component Enterprise Architectures. The Program Management Plan shall also identify milestones towards its completion. The EAPMO Program Management Plan shall address this recommendation by the end of December 2006.

**Recommendation 2.**

*Provide Departmental Guidance to components for the development and maintenance of Enterprise Architectures consistent with the guidance provided by the Federal Enterprise Architecture Framework, the OMB, and the GAO.*

**Concur.** The EAPMO Program Management Plan will provide for explicit mechanisms to coordinate with and provide guidance to Components for the development and maintenance of their Enterprise Architectures. The Program Management Plan will



**Concur.** The EAPMO Program Management Plan will provide for explicit mechanisms for tracking and reviewing the planning, development, completion, and updating of component-level Enterprise Architectures. This shall be done in a way to leverage and complement, not replace, existing oversight activities. The EAPMO Program Management Plan shall address this recommendation by the end of December 2006.

**Recommendation 4.**

~~Fully implement the phases outlined by the ITSM framework to ensure that all Department IT investments are covered by an ITIM process.~~

ITSM processes  
received feedback  
currently re-  
on lessons  
rtment will  
~~schedule to~~  
nts.

**Concur.** In FY05, the Department executed several ITSM processes from the first two phases of the framework, and received feedback from partners and participants. The Department is currently evaluating and updating the ITSM framework based on lessons learned. By the second quarter of FY06, the Department will complete the updates to the ITSM framework, and implement the remaining processes across all investments.

**Recommendation 5.**

develop them.

*Ensure that Components requiring ITIM processes develop them.*

Component ITIM  
, percent of  
f the third

**Concur.** The Department will define the need for Component ITIM processes based on criteria such as size, mission need, enterprise investment dollars, etc. By the end of FY06, the Department will have defined the need for Component ITIM processes across all investments.

**Recommendation 7.**

*Establish a clear schedule for the completion of the ITSM Framework and the completion of a mature ITIM process.*

**Concur.** The Department will develop a schedule by the end of January, 2006.

## OFFICE OF THE INSPECTOR GENERAL'S ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE REPORT

Pursuant to the OIG's standard audit process, the OIG provided a draft of this audit report to the Department of Justice on September 26, 2005, for its review and comment. The Department's October 20, 2005, response is included in Appendix 10 of this final report. The Department concurred with all seven recommendations in the audit report. Our analysis of the DOJ's response to the seven recommendations is provided below.

### Status of Recommendations

1. **Resolved.** This recommendation is resolved based on the Department's agreement to complete a Department-wide Enterprise Architecture. This recommendation can be closed when we receive documentation demonstrating that the Department has completed an organization-wide Enterprise Architecture.
2. **Resolved.** This recommendation is resolved based on the Department's agreement to provide guidance to components for the development and maintenance of Enterprise Architectures. This recommendation can be closed when we receive documentation demonstrating that the Department has issued guidance to its components for the development and maintenance of Enterprise Architectures.
3. **Resolved.** This recommendation is resolved based on the Department's agreement to track and review the planning, development, completion, and updating of component-level Enterprise Architectures. This recommendation can be closed when we receive documentation demonstrating that the Department is tracking and reviewing the plans, development, completion, and updating of component-level Enterprise Architectures.
4. **Resolved.** This recommendation is resolved based on the Department's agreement to fully implement the phases outlined by the ITSM framework to ensure that all Department IT investments are covered by an ITIM process. This recommendation can be closed when we receive documentation demonstrating that all Department IT investments are covered by an ITIM process.
5. **Resolved.** This recommendation is resolved based on the Department's agreement to ensure that its components requiring

ITIM processes develop such processes. This recommendation can be closed when we receive documentation demonstrating that the Department has ensured that its components requiring ITIM processes have developed such processes.

6. **Resolved.** This recommendation is resolved based on the Department's agreement to provide assistance to its components in developing and implementing ITIM processes and providing value-added services. This recommendation can be closed when we receive documentation demonstrating that the Department has provided assistance to its components in developing and implementing ITIM processes.
7. **Resolved.** This recommendation is resolved based on the Department's agreement to establish a clear schedule for the completion of the ITSM Framework and the completion of a mature ITIM process. This recommendation can be closed when we receive documentation demonstrating that a schedule has been established for the completion of the ITSM Framework and the